nsdクイックセットアップ

2015/03/11
DNSサーバに nsd を使う設定メモ。FreeBSDのports からのインストールなので。tarballからの細かい作業はすっ飛ばしてある。

プライマリDNSサーバを走らせていた仮想マシンをメンテするため、別のセグメントにセカンダリDNSサーバを立ち上げした。

手順

ドメインは hogehoge.jp を仮定している。
OS環境はプライマリ・セカンダリ ともに FreeBSD 10.1 64bit版で、コンテンツサーバ nsd を使用している。

1. セカンダリDNSを実行するサーバにnsdをインストール
2. プライマリ/セカンダリのnsd.conf修正
3. 契約業者のネームサーバへ登録

インストール

portinstall なり cd /usr/ports/dns/nsd; make install なりで済ます。このドキュメント作成時点では nsd 4.1.1 がインストールされる。 nsd実行アカウントユーザ nsd。グループ nsd が作成される。

インストールが済んだら以下を /etc/rc.conf に追加する。

```
nsd_enable="YES"
```

次に、nsd-control-setup の実行を行い証明書を生成する。nsd-controlコマンドを使うためこれは必須。

nsd.conf の設定

/usr/local/etc/nsd/nsd.conf.sample があるので、こちらを/usr/local/etc/nsd/nsd.conf へコピーし、編集する。

以下記述は必要な部分だけ集めたもの。 定義中、プライマリサーバは aaa.bbb.ccc.ddd 。セカンダリサーバは www.xxx.yyy.zzz のIPアドレスとする。

プライマリ側

既にプライマリでも nsd が運用されていた場合。nsd.conf でセカンダリサーバへのサーバへ通知について定義する。

nsd.conf

```
server:
    ip-address: aaa.bbb.ccc.ddd
    logfile: "/var/log/nsd.log"
    hide-version: yes

remote-control:
    control-enable: yes

pattern:
    name: "myzone"
    zonefile: "%s.zone"
    notify: www.xxx.yyy.zzz NOKEY
    provide-xfr: www.xxx.yyy.zzz NOKEY
    notify-retry: 5
    outgoing-interface: aaa.bbb.ccc.ddd
```

nsd-controlコマンドで定義するので zone セクションは定義していない。

セカンダリ側

nsd.conf でプライマリサーバの通知を受け付ける定義を実施する。

nsd.conf

```
server:
    ip-address: www.xxx.yyy.zzz
    logfile: "/var/log/nsd.log"
    hide-version: yes

remote-control:
    control-enable: yes

pattern:
    name: "myslavezone"
    zonefile: "%s.zone"
    allow-notify: aaa.bbb.ccc.ddd NOKEY
    request-xfr: AXFR aaa.bbb.ccc.ddd@53 NOKEY
    allow-axfr-fallback: yes
    outgoing-interface: www.xxx.yyy.zzz
```

nsd-controlコマンドで定義するので zone セクションは定義していない。

request-xfrの定義で@53をつけているのはポートを明示したほうがいいよ、という話しがあったため。
無しで動作するなら@53は消してもよいかも。

nsd実行

セカンダリ側のnsdを起動。

```
root@amane # service nsd start
Starting nsd.
root@amane #
```

プライマリ側のnsdを再起動。

```
root@sakura # service nsd restart
Stopping nsd.
Waiting for PIDS: 5750.
Starting nsd.
root@sakura #
```

セカンダリサーバでの初回登録が行われていない状態だとプライマリサーバの /var/log/nsd.log に

```
[2015-03-11 hh:mm:ss.sss] nsd[5750]: error: xfrd: zone hogehoge.jp: received
notify response error NAME ERROR from www.xxx.yyy.zzz
[2015-03-11 hh:mm:ss.sss] nsd[5750]: error: xfrd: zone hogehoge.jp: received
notify response error NAME ERROR from www.xxx.yyy.zzz
[2015-03-11 hh:mm:ss.sss] nsd[5750]: error: xfrd: zone hogehoge.jp: received
notify response error NAME ERROR from www.xxx.yyy.zzz
[2015-03-11 hh:mm:ss.sss] nsd[5750]: error: xfrd: zone hogehoge.jp: received
notify response error NAME ERROR from www.xxx.yyy.zzz
[2015-03-11 hh:mm:ss.sss] nsd[5750]: error: xfrd: zone hogehoge.jp: received
notify response error NAME ERROR from www.xxx.yyy.zzz
[2015-03-11 hh:mm:ss.sss] nsd[5750]: error: xfrd: zone hogehoge.jp: max
notify send count reached, www.xxx.yyy.zzz unreachable
```

と怒られるので、初回だけセカンダリサーバでaddzoneする必要がある。

nsd.confと同じディレクトリに、プライマリサーバのゾーンファイルをコピーし、nsdへ登録する。このゾーンファイルはBINDで作るものと同じ書式。以下は作業で使った例。

hogehoge.jp.zone

```
$TTL 3600
@               IN      SOA     name.hogehoge.jp. root.hogehoge.jp. (
                                2015031101      ;serial
                                10800           ;refresh
                                3600            ;retry
                                604800          ;expire
                                600 )           ;negcache
;
                IN      NS      name.hogehoge.jp.
                IN      NS      name2.hogehoge.jp.
;
```

```
localhost       IN      A       127.0.0.1
;
@               IN      MX      10   mail.hogehoge.jp.
;
@               IN      A       mmm.nnn.ooo.ppp
name            IN      A       aaa.bbb.ccc.ddd
name2           IN      A       www.xxx.yyy.zzz
mail            IN      A       mmm.nnn.ooo.ppp
```

nsd-controlコマンドの addzone サブコマンドで hogehoge.jp.zone を登録する。

```
root@amane # nsd-control addzone hogehoge.jp myslavezone
ok
root@amane #
```

必要なら逆引きのゾーンファイルも同じように登録する。

その後はプライマリサーバ側でゾーンの情報が修正されるとその内容がセカンダリサーバへ転送される。
たとえばゾーンファイルのシリアルが 2015031101 から 2015031102 に変更されていれば、セカンダリサーバの /var/log/nsd.log に

```
[2015-03-11 hh:mm:ss.sss] nsd[5596]: info: zone hogehoge.jp serial
2015031101 is updated to 2015031102.
```

が記録され、変更内容が転送されている事がわかる。

業者のネームサーバへ登録

セカンダリサーバを hogehoge.jp のネームサーバとして登録する。この設定は契約している業者により異なると思う。
うちの場合は name.hogehoge.jp(aaa.bbb.ccc.ddd) と name2.hogehoge.jp(www.xxx.yyy.zzz) を登録した。

hogehoge.jp.zoneに定義した nameとname2は、業者のシステムで要求しているため。

業者側のDNSに反映が行われたら（最短でも1日くらいかかるかと）、短時間プライマリ側のサービスを停止してdigコマンドやdrillコマンドで名前解決が出来ることを確認する。
セカンダリ側が機能しているようなら成功。

DNS, nsd, 技術資料