bind 9への移行ガイド(初級編) NISOC版

2005/09/03
神保道夫
karl@nisoc.or.jp

きっかけ

- FreeBSD 5.3-RELEASEから、bindが8→9になったことにより、設定・運用が微妙に変わった。
- ここでは、FreeBSDでの運用方法のtipsを紹介する。

/etc/namedb ディレクトリ

- /etc/namedb が、/var/namedb/etc/namedbのsymbolic linkに変更され、/var/namedbがchrootディレクトリしやすくなった。

namedの起動・終了

- FreeBSDでは、/etc/rc.d/named startで起動、/etc/rc.d/named stopで終了する。
- ただし、/etc/rc.confでnamedの起動パラメータが正しく指定されていれば有効になる。

namedのバージョンを調べる

- BIND 8.2.2-T4B以降は以下のコマンドでバージョンを調べることができる
  5.3-RELEASEの場合
  #named -v
  BIND 9.3.0
  5.4-RELEASEの場合
  #named -v
  BIND 9.3.1
- あるいは、起動時のsyslogの出力を見るとわかる

古いnamedの危険性

- bind 4や8を用いている場合、DNSリクエストのforwarder(サーバ内に情報がない場合、他のサーバに問い合わせを行う機能)を使うように設定されている状態では、**「DNSキャッシュ汚染」**(勝手に悪質な偽のサイトへとリダイレクトしてしまう)脆弱性が存在する。そのため、最新のbindをインストールすることをお勧めする。

rndcコマンドとの協調

- rndcとは、remote name daemon controller の略で、リモートサーバーからnamedを制御するコマンドです。FreeBSDのnamedを起動し、named.confにcontolsステートメントがなく、rndc.confファイルがない場合は、localhostのnamedを制御することが可能です。

rndcの利用例

- namedを再起動せずにゾーンデータを変更する
  rndc reload nisoc.or.jp
- namedを再起動せずにゾーンを追加・削除する
  rndc reconfig

nslookupコマンド

- 昔からある、DNSの設定を検索するコマンドです。
  ・コマンドラインからダイレクトに検索することも、対話式に検索することも可能である
  ・Windows 標準のコマンドとして付属している事
- などから、必ず覚えておくと良いコマンドとも言えます。

digコマンド

- dig(domain information groper)コマンドは、従来のnslookupコマンドの代わりとして推奨されているコマンドです。
- dig @127.0.0.1 a www.example.co.jp
  localhostのnamedに対して、www.example.co.jp のAレコードを検索する
- dig @127.0.0.1 -x 192.168.0.1
  localhostのnamedに対して、192.168.0.1のPTRレコードを検索する

hostコマンド

- とりあえず、ホスト名やIPアドレスがわかればよいという場合は、hostコマンドが非常に便利です。例えば、以下の様に使えます。

```
#host sv.example.jp.
sv.jinbo.jp has address 210.229.61.162
sv.jinbo.jp has IPv6 address 2001:200:523:1::1
sv.jinbo.jp mail is handled by 0 sv.example.jp.
#host 210.229.61.162
162.61.229.210.in-addr.arpa is an alias for 162.160.61.229.210.in-addr.arpa.
162.160.61.229.210.in-addr.arpa domain name pointer sv.example.jp.
#host -i 2001:200:523:1::1
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.3.2.5.0.0.0.2.0.1.0.0.2.ip6.int domain
name pointer sv.example.jp.
```

最近のtopics(1)

- DNSサーバーの不適切な運用により、ドメインの乗っ取りが可能な状態になるケースが多々ある。(ex. visa.co.jp事件など)
- http://www.e-ontap.com/summary/ などに、詳しい経緯や、対策方法が載っているために、このサイトを是非参照してほしい。

最近のtopics(2)

- このようなDNSサーバーの不適切な設定に対して、JPRSでもDNSサーバの不適切な管理による危険性解消のための取り組みを開始
  http://jprs.co.jp/press/050804.html
- 国内の属性型・汎用JPのドメインについては、指定事業者がチェックできるような仕組みを用意(ただし、指定事業者が管理できるドメインに限る)

最近のtopics(3)

- このような、DNSサーバーの不適切な設定を自動で調べてくれるサイトもある
- 例
  http://www.dnsreport.com/

まとめ・参考文献等

- named が8→9になって、若干構文が変わったりしたコマンドもあるが、named 4→8への変更よりも少ないため、覚えるのは比較的簡単です。
- 詳しくは、DNS&BIND クックブックや、DNS&BIND 第4版をご覧ください。