IPv6対応で考えないといけないこと

(という内容で申し込んだけど別のネタを思いついた)

2011/11/30 dnsops.jp BoF
Kazunori Fujiwara, JPRS
<fujiwara@jprs.co.jp>
dnsops.jpに登録したアドレスは<fujiwara@wide.ad.jp>

赤枠内に若干追記しました
2011/12/5

別ネタ: BIND 9バグの根本的対策

- Authoritative server
  - 2台以上にし、Master, SlaveをBIND 9, NSDで動かす
  - 同時に落ちなければよい
- Full-Resolver
  - BIND 9, Unboundの二つ動かす (同じマシンでもよい)
    - Private addressならいっぱいあるし、127.0.0.2も使用可能
  - ユーザには二つのアドレスを通知
  - isc-dhcpd: option domain-name-servers に両方書く
  - /etc/resolv.conf にname server行を二つ書く
  - 一つ目が停止しても、気になる遅延なし　(4台しらべたうちの4台: FreeBSD 8.2, WindowsXP, 7, Debian)
    - digは遅くなり、WindowsXPのnslookupはエラーになるが
- 適度に監視する
- これで、”重複をお許しください”にあせる必要なし！
  - BIND 9のセキュリティ問題はサービス停止がほとんどだから

逆引き設定

- IPv4では、日本のISPはユーザに動的割り当てしたアドレスの逆引きを機械的に登録している
  - 逆引きがあることを前提とした設定が多い
- 大昔、APNICがIPv4の逆引き設定を失敗して、多くのゾーンの逆引きが消えたときに多くの悲鳴が聞こえた
  - 質問: これはほんと？
  - janogとかのメーリングリストではみかけたけど
- なにが起きたか教えてください
  - ssh loginに時間がかかる？
  - メールが送れない？
  - 掲示板などの投稿規制が動かない　(森下さん情報)

/etc/hosts.allowにドメイン名を書いていて、入れなくなった事例があるそうです

IPv6での逆引き

- ユーザネットワークには最小で/64, 64bit, 2の64乗個のアドレスが割り当てられる
  - すべてのアドレスに逆引きを設定することは困難
    - 解決策はあるが、やろうとしてるひとは少ない
      - 定型ホスト名を自動生成 v6rev.pl (拙作)
      - dhcpv6, NDを監視して逆引き登録とか
      - すべてのエンドノードがdynamic update
  - エンドノードの使うアドレスはときどき変わる (毎日?)
    - RFC 4941 Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- 現在、エンドノードの逆引きはないことが多い
  - サーバの逆引きは付けるもの

サーバでの逆引きの現状

- サーバ系での逆引きはIPv4と同じ
  - IPv6だけ特別扱いはしない
  - IPv4, v6で共通にon/offするしかない
- sshd
  - 認証時の補助(.shosts, authorized_keysのfrom=)
  - who, lastlogなどで表示するためだけに使用？
- メール
  - SMTP: メールサーバ間では必須
    - 相手が受け取ってくれない
    - IPv6でもメールサーバの逆引きは必須
  - Submission: クライアント-メールサーバ間
    - SMTPAUTHするから不要で、なくてもよいようにしてますよね？
- Web:　逆引きすると遅くなるから、普通はしない?
- IRC: 逆引きするが、IPアドレスでのACLあり

/etc/hosts.allowのドメイン名に注意
sshd_configのドメイン名に注意

サーバでのおすすめ

- サーバマシンのアドレスには逆引きを設定する
- サービスごとに逆引きをon/offする
- sshd: 必要がなければoffにする
  - -u0 , usedns no
  - ホスト名認証を使っている場合はIPアドレスに変更
- submission server, http server: 逆引きoff
- 投稿規制は、IPv6アドレスベースで実現する
  - ISPや組織単位だと/32とか/48, その単位でNS引いてもいいけど
  - エンドユーザだと/64単位？
- ログの集計プログラム
  - IPv6アドレスのprefix /32, /48ごとに接続元を分類する
    - /32, /48のNS RRを引くとだいたい組織がわかる？
  - クライアント数はIPアドレスごと

/etc/hosts.allowには、ドメイン名を書かない
sshd_configも同様

RegistrarのIPv6, DNSSEC対応

- ドメイン名を登録しても、DNSサーバのIPv6アドレスを設定できないとIPv6対応できません
  - DNSSECも同じ
  - 対応していることを確認してから登録しましょう
- 対応しているレジストラ・リセラ情報を持っている人はいらっしゃいますか？
  - gTLDだと、Go DaddyはIPv6, DNSSECともに登録可能
    - NetworksolutionsはIPv6についてはメールを送るとできるそうだ
  - JPだとjpshop.jpに情報あり (最新情報は直接聞いて)
- 情報集めませんか？

「ipv6 registrar」でgoogle検索するといくつか情報があります
ARINの以下のページが、おそらく更新されていないけどよいです
http://getipv6.info/index.php/DNS_Registrars_IPv6_Support_Status

まとめ

- BIND 9とNSD, Unboundを組み合わせればBIND 9が落ちても問題なし
- 逆引きが壊れたときの事件教えてください
- IPv6では、逆引きがないアドレスが多いので、それを前提にサーバの設定を考える必要があります
- レジストラ・リセラのIPv6, DNSSEC対応状況を収集・共有しませんか？