WindowsキャッシュDNSサーバ
と
社内情シスの私

株式会社ブロードバンドタワー
大本　貴

- 職歴
  - 2000年 インターネット総合研究所入社
  - 2001年 プロデュースオンデマンド(PoD)に出向
    - ストリーミング配信技術担当
  - 2007年 インターネット総合研究所に帰任
    - 主に社内情報システムのサーバ・ネットワーク運用、コンサルなど
    - 2010年春からDNSSECジャパンの活動に参加
  - 2010年 ブロードバンドタワーに転籍
    - DNSSECジャパンの活動終了に伴いDNSOPS.jpの活動に合流

twitterでたまにDNSSEC関連のつぶやきをしています。

@taxiJPN

こんなカバンで街中

ほっつき歩いてます。→

社内情シス担当の皆さん、

キャッシュDNSサーバは、どのソフトウェアをお使いですか?

- 社内ネットワークというと、
  多くの企業で利用されているのが、

Active Directory

- Active Directoryを導入しているなら必須なサービス、それが

Windows

DNS サービス

AD認証機能で利用する内部ドメインの構成にもよりますが、AD認証対象となるドメインの権威DNS兼キャッシュDNSサーバとするのが一般的ですよね?

(決してMSの回し者ではありません。)

BroadBand Tower, Inc.

そして、大丈夫ですか?

2015/7/14

Windows Server 2003は
MSサポート終了しました。

アップグレードを考える。

- server2003　→　server2008 R2
  - 延長サポート2020/01/14まで
- server2003　→　server2012 R2
  - 延長サポート2023/01/10まで

- server2008を選択する主観的メリット
  - server2012のメトロUIインターフェイスが、くっそ使いにくくて作業がはかどらない!　(※個人の感想です)
  - サポートまだ5年あるし、2012の次(2016)は、もうちょっと使いやすいの、出るかな?
- server2012を選択する主観的メリット
  - ADが完全仮想化出来るようになったとか。
  - DNSSEC対応がようやくまともになったとか。(R2)

- で、2014年の春に私の取った選択としては、

まだ6年以上サポート期間あるし、2008R2にアップグレードや!

2012は自分一人で運用するだけでもしんどいのに、チーム全体の練度を考えると生産効率落ちすぎで使えるかいいい!

～プロローグ　完～

そして本題へ

- server2008R2を導入して半年経過。

- ある社員から問い合わせが。

社員A「なんか、あるお客さんのドメインだけが名前解決できないんだけど?」

状況整理

- お客さんのドメインはexample.biz (仮)
- 主要なTLDのうち、.bizなドメインだけが名前解決できない。.comや.jpなどのドメインの名前解決は正常動作。
- よくよく調べるとexample.bizだけでなく、他の***.bizも名前解決できない。というか.bizのNSすら・・・。
- ただし、社内キャッシュDNSサーバを介さずに8.8.8.8などに問い合わせると.bizの各ドメインも名前解決できる。
- 社内キャッシュDNSサーバはDNSSEC非対応。(server2008はNSEC3非対応だったりするので。)

- 色々調べてみると、MSの公式フォーラムの記事にたどり着いた。

- **Server 2008 DNS not caching .biz**
- https://social.technet.microsoft.com/Forums/windowsserver/en-US/cde90577-0e42-40b5-b3c3-8f348805d2ad/server-2008-dns-not-caching-biz

Server 2008 DNS not caching .biz

BroadBand Tower, Inc.

- 2010年のMS公式フォーラムでの記事

- 投稿者たちの発言を要約すると、
  - やはりserver2008のWindows DNSサービスでは.biz は名前解決できないことがある。**が、原因は分からない。**
  - ただし解決方法としてはこの記事内で2つの手法が提示されている。
    - **EDNS0を無効化する。**
    - **フォワーダー設定に*.bizの名前解決は8.8.8.8などにフォワードする設定を入れる。**

- **え、EDNS0が関係するの?!**
  - ファイアウォールが512byte以上のUDPパケットを叩き落す事例もあるらしい。
  - だが、.bizのNSレコードをdigると 302byte
  - だが、当該server2008上からはnslookupできない。
  - そもそもファイアウォールが問題ならば、他のTLDも名前解決できないはず。
- **じゃあTCPフォールバックは?**
  - WireSharkでパケットを見ている限り、少なくとも問題のクエリについては、どうやらTCPフォールバックせずにServer failed判定しているように見える。

- 社内ネットワーク内ではDNSSEC対応予定はまだない。ので、試しにEDNS0を無効化してみた。
  - 確かに*.bizの名前解決ができるようになった。
- 残る疑問
  なぜEDNS0とserver2008と*.bizの組み合わせだけなのか。
  - EDNS0が問題ならば、512byteを超えてないのに、EDNS0が関係するのか?
  - もしDNSSEC周りが問題ならば、.jpや.comなドメインなどでも現象が発生してもおかしくない。
  - DNSSEC対応している8.8.8.8でも現象が出ておかしくないのでは?
- 納得いかないが、すでに社内では騒ぎになっているし、復旧を優先し、これで乗り切ることとした。

- と、ここで終わってもネタ的に浅いので、Windows Server2012をセットアップして検証してみた。
  - Server2012、Server2012R2のいずれも問題再現せず。
  - ちなみにserver2003でも問題再現しませんでした。

- もちろんbindやunboundでも再現せず。

まとめ

- ということで、server2003からの乗り換えは、メトロUIが辛くとも、server2012R2への乗り換えをお勧めします。
- でも、なんでEDNS0無効化で解決できたんだろうか・・・。納得できないが、社内情シスの立場として、これ以上運用しているシステムを巻き添えにして深追いする余裕もない。興味のある誰かが追ってくれるだろうことを期待しよう。

ま、ともかく、

暫定復旧したWindows2008先生の今後にご期待ください的

完

・・・・と、思っていたら、更に数か月後。

別の社員から問い合わせが。

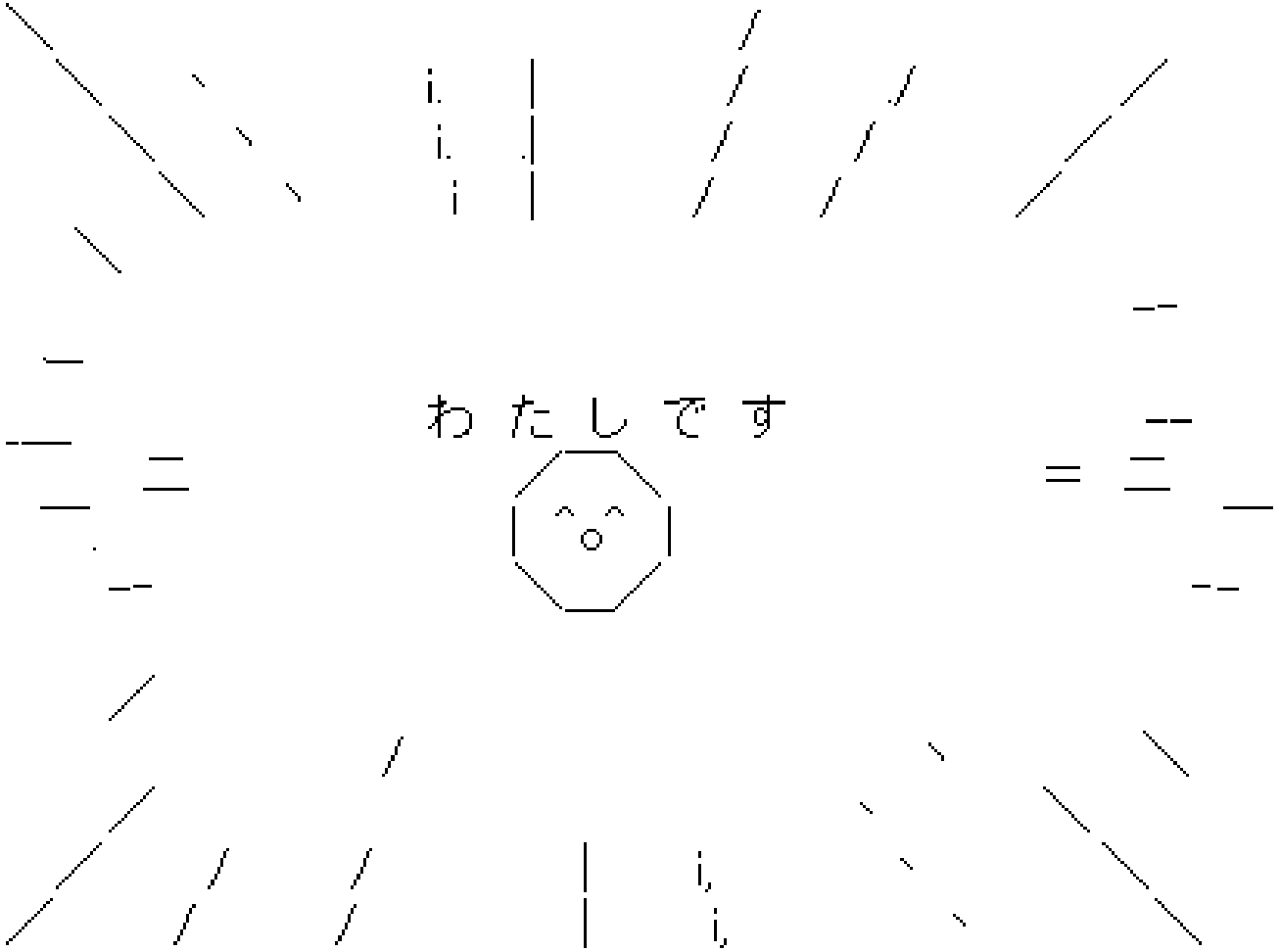
社員B「なんか、あるお客さんのドメインだけが
名前解決できないんだけど。」

え、何このデジャヴ感。

ま、まさか・・・・(**ゴゴゴゴゴ・・・**)

He came back….

社員B「*********.bizです。」



- **キャッシュDNSサーバの設定を再確認。**
  - レジストリを確認してもEDNS0は無効設定のまま。
  - つまり、EDNS0(とか512byte以上とかDNSSEC)はどうやら**無罪**。
  - 挙動を更に追跡して見ると、どうも*.bizのNSである、*.gtld.bizのAレコードのTTLが切れた時に、Aレコードの更新問い合わせをせずにそのままネガティブな状態を保持し続けているっぽい
  - (が、事象発生間隔から、複数の要素がトリガーな可能性もある。もしかすると、AレコードのTTLが切れている、かつNSレコードのキャッシュが有効なまま存在している時か?)
  - ただ、Cacheバグに関するパッチは昨年server2008を構築した時点ですでに導入済み。
    - Windows Server 2008 R2 の DNS サーバー サービスは、しばらく正常に動作した後、一部の外部 DNS 名を解決しません。
      https://support.microsoft.com/en-us/kb/2508835/ja

その後

- **もう一つの回避策、で条件付きフォワーダーに設定投入。**
  名前解決できない*.bizをを8.8.8.8に転送問い合わせする設定。
  再度*.bizの名前解決できるようになった。暫定復旧。

- **その後、フォワーダー設定を消去し、現在こちらのパッチで経過観察中。**
  - Windows Server 2008 and Windows Server 2008 R2 DNS Servers may fail to resolve queries for some top-level domains
  - https://support.microsoft.com/en-us/kb/968372
    - レジストリのMaxCacheTTL値をdefaultの1日から2日以上に伸ばす処置。
    - 「.co.uk、.br、.cnで起きている現象への対策パッチだが、前述のドメインに限らない」と書いてあるのでもしかすると.bizもこれか? 報告されている現象も酷似している。
    - ちなみにco.ukや.brのNS、Aレコード周りのTTLは2日
    - .bizのNSとa.gtld.bizのAレコードは@*.gtld.biz上は6日、root-serversは2日
    - gtld.bizのNSレコードのTTLは2時間
    - なのに、server2008のキャッシュDNSサーバを介してgtld.bizのNSレコード(キャッシュ済み)を問い合わせると、キャッシュクリア直後は2時間なのに、しばらくするとTTL3日以上の値が返ってくることがある。 あらやだ、何これ。

再度のまとめ

- というような苦労もあるので、server2003でActive Directory をまだお使いの方はserver2012R2への乗り換えおすすめ。
  - (もちろん、2012は2012でDNS周りの修正パッチがいくつか出ているので注意は必要ですが・・・。)

- server2008を使う(使っている)ならキャッシュDNS周り見直してみてください。(今把握しているのは.bizだけですが、新gTLDとか考えると震える。。。)
  - dnscmd /clearcache コマンドをバッチで定期実行するとかも検討してみてください。
  - Windows DNSサービスに加えてフォワーダー用キャッシュDNSサーバをunboundなどで別建てすることをおすすめ。(その費用が出ないなら8.8.8.8へ・・・)

おしまい

より良い社内情シス運用ライフを!