

Unboundの

追加パラメーターチューニング

IIJ

Internet Initiative Japan

株式会社 インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation



3年前(2016年) DNS Summer day

<https://dnsops.jp/event/20160624/unbound.pdf>



3年前(2016年) DNS Summer day

これだけは変更しておけパラメータ (ISP)

- libeventの利用(compile時)
 - fd 1024個制限の突破
- num-threads (デフォルト1)
 - CPU個数と同じに (自動検出してよ…)
- incoming-num-tcp (デフォルト10(低すぎ…))
 - TCPクエリ数に応じて。1000くらい?
- outgoing-num-tcp (デフォルト10(低すぎ…))
 - 水責め攻撃に加担しているclient数に応じて
 - 権威DNSサーバー(UDP)が詰まる→TCPで聞く→TCPも詰まる→こっちも詰まる
 - 1000くらい?

3年前(2016年) DNS Summer day

これだけは変更しておけパラメータ (ISP)

- num-queries-per-threads (デフォルト1024)
 - QPSに応じて
- outgoing-range (デフォルト4096)
 - num-queries-per-threadsの2倍にする
- net.core.rmem_max, rmem_default
 - カーネルパラメータ
 - 適当に、4 or 8MBくらいらしい

追加項目のお話

常識だったらゴメンね (・ω<)☆

ある日の問い合わせ

お客様「XXX.gov.xxのMXの名前解決が遅い」
私（権威DNSサーバのうちのいくつかが落ちたりして
るだけでしょ…）

もうちょっと調べてみた

- NSレコードに4ホスト書いてある
- どのホストもA/AAAA両方が書いてある
- すべてのAAAAレコードが応答がない

IPv6の扱いとは…

⇒ v6で4回名前解決失敗してから、v4で成功している (prefer-ipv6: yesだからかも)

- MXのTTLが20秒, NSのTTLが60秒

おかしい・・・

- 初回が遅いのはわかるけど
- TTL分過ぎると、また遅い
 - 最初から引き直している
- おかしくね？

これ、なんていうの？(DNS用語で)

- BINDもUnboundも(他の実装もでしょう)、各権威DNSサーバのIPアドレス毎に、応答のある・なし、RTTなどをcacheしている

```
$ unbound-control dump_infra
210.130.0.5 iij.ad.jp. ttl 871 ping 0 var 56 rtt 224 rto
224 tA 0 tAAAA 0 tother 0 ednsknown 1 edns 0 delay 0 lame
dnssec 0 rec 0 A 0 other 0
```

```
$ rndc dumpdb -adb      # Address database dump
; 210.130.1.5 [srtt 5] [flags 00000000] [edns 0/0/0/0/0]
[plain 0/0] [ttl 1743]
```

infra-host-ttl

これをcacheする時間のパラメータが

```
infra-host-ttl: <seconds>
```

```
Time to live for entries in the host cache. The host cache contains roundtrip timing, lameness and EDNS support information. Default is 900.
```



おかしい…。900秒はv6アドレスには疎通がないことを覚えているので、いきなりv4アドレスに聞きに行くはずでは・・・

unbound.confのdocumentを読むと もう一つ見つけた

```
infra-cache-numhosts: <number>  
Number of hosts for which information is cached.  
Default is 10000.
```

生存時間は…？

定期的にdump_infraしてみた

⇒ デフォルト(10,000):

なんとということでしょう、

1分未満で揮発していました。



これやん

増やしてみた

- 10倍(100,000): 7分未満で揮発
 - デフォルトTTLが900秒 = 15分 なので、まだ足りない
- 100倍(1,000,000): 15分少々で揮発
 - ⇒ なんとか大丈夫そう
- 百万でdumpすると、textで17MBとか
- RESが16.7GB ⇒ 17.5GBくらいに増加

まとめ

高QPSなUnbondでは、
infra-cache-numhostsも増やしましょう

具体的な値は計測しましょう

QPSやNSホスト数によって変わる(ハズ)

余談

Unboundの悩ましいところ?

- RD bitの立っていないクエリに応えない
 - dig +trace ... するときに困る
 - ユーザが普通に使う分には全く困らない
 - はじめのクエリ(“.”のNSの検索)をresolv.confのIPアドレスにRD bit無しで投げるため
 - access-controlの第二パラメータにallowの代わりにallow_snoopと書くと応答する

```
access-control: 192.0.2.0/24 allow
```

↓

```
access-control: 192.0.2.0/24 allow_snoop
```

- dig @a.root-servers.net +trace ... する
- drill -T ... する (root-serversに直接聞く)

余談

digのbugということで、
直ったそうなの

めでたしめでたし。



<https://twitter.com/hdais/status/1143483713151365120>