Unboundの追加パラメーターチューニング

IIJ
Internet Initiative Japan

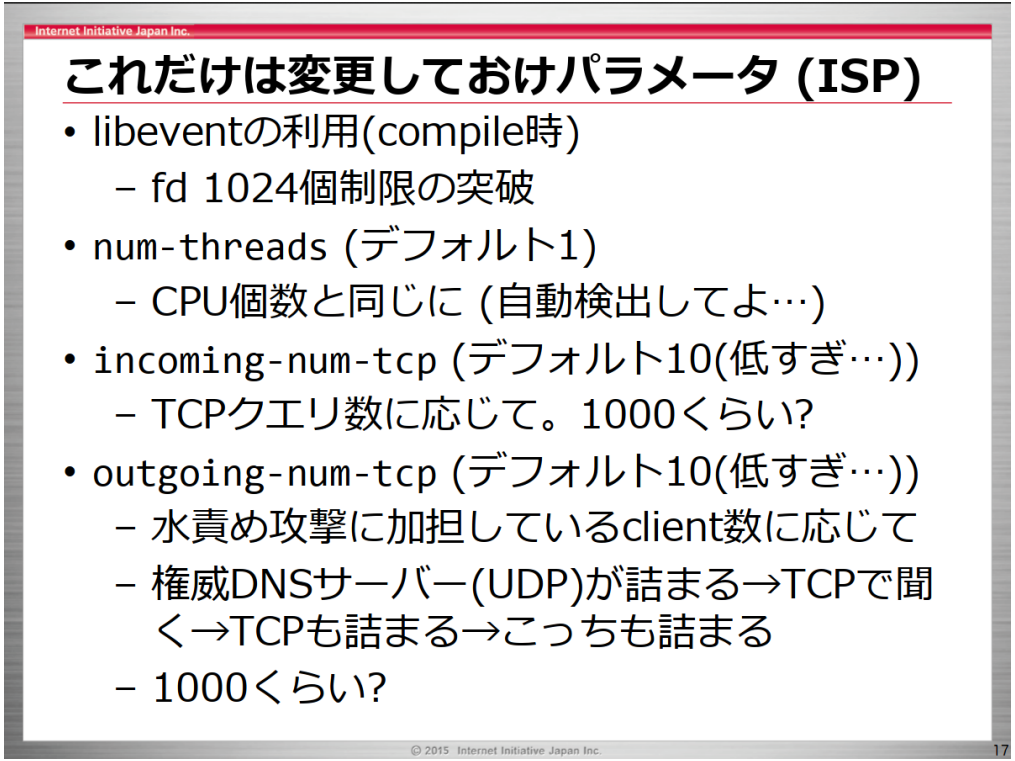
株式会社 インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

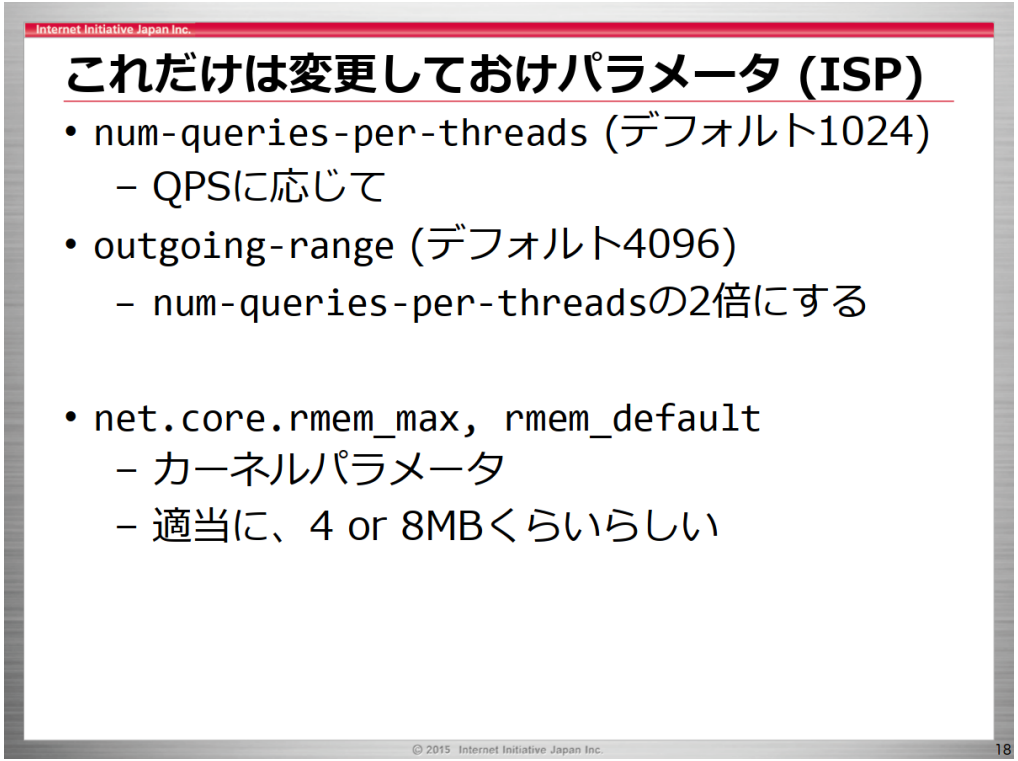
3年前(2016年) DNS Summer day

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

3年前(2016年) DNS Summer day



3年前(2016年) DNS Summer day



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 con-
 tains 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

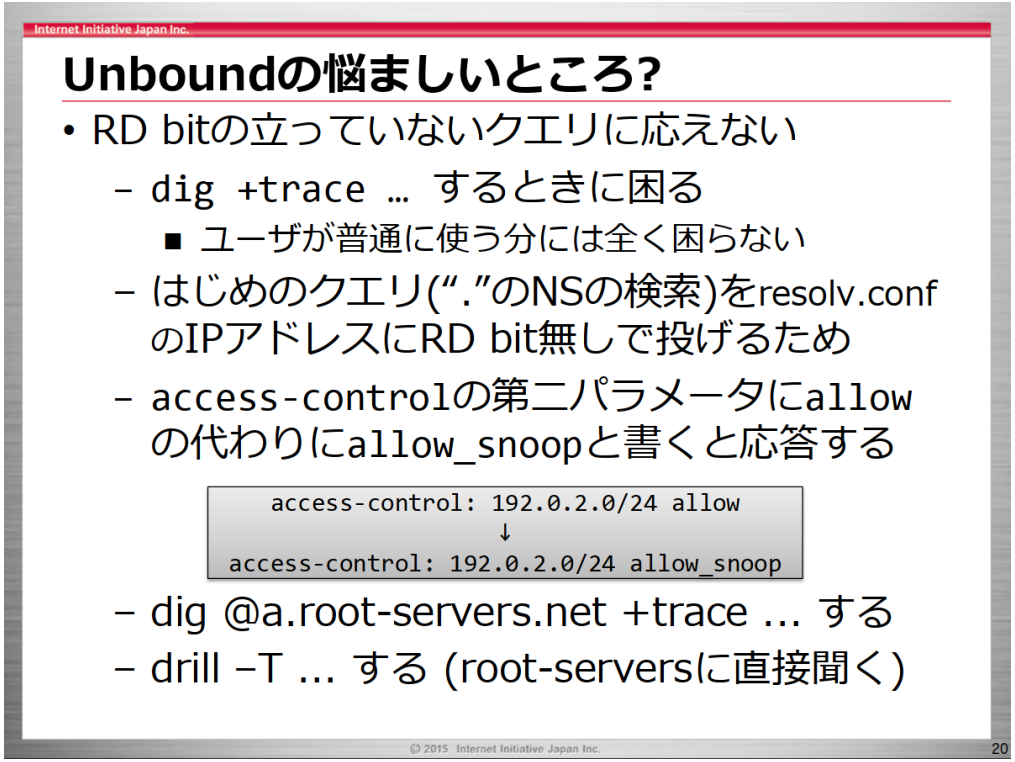
  ⇨ なんとか大丈夫そう
- 百万でdumpすると、textで17MBとか
- RESが16.7GB ⇨ 17.5GBくらいに増加

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



余談

digのbugということで、
直ったそうな

めでたしめでたし。

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