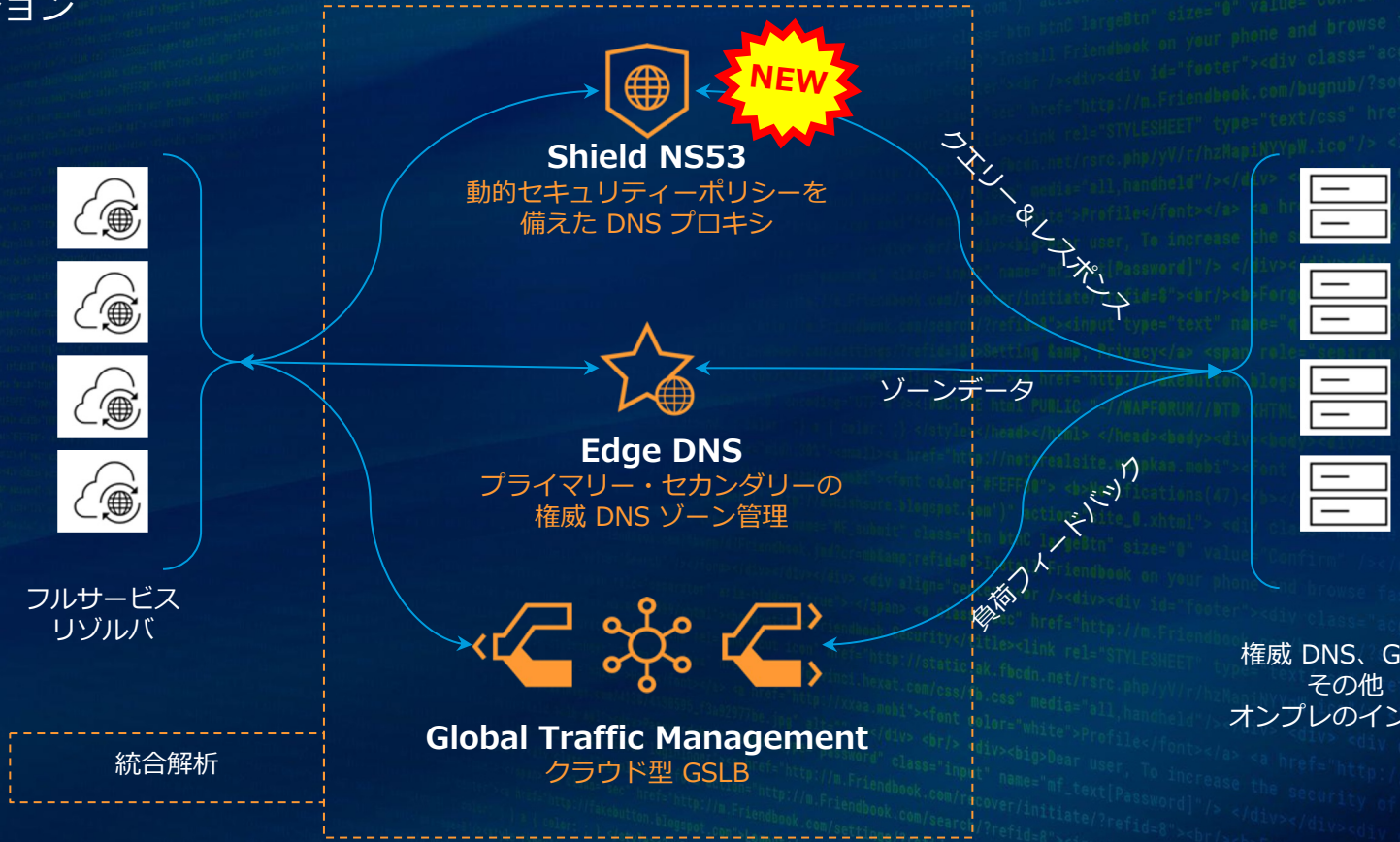
アカマイの権威 DNS サービス / あたらしかった dig

アカマイ・テクノロジーズ合同会社
シニア・ソリューションズ・エンジニア
松本 陽一

アカマイの権威 DNS サービス

世界で最も分散された Akamai Connected Cloud 上に数千台のサーバーで構成された権威 DNS ソリューション



Edge DNS
プライマリー、セカンダリーの権威ゾーンデータ管理

- 最大規模の DDoS に対してもパフォーマンスと可用性を継続的に確保できるように設計された権威 DNS サービス
- GUI、API、ゾーン転送による柔軟なゾーンデータ管理
- 詳細なトラフィックレポート、ログの提供
- 自動化された DNSSEC の鍵管理と署名
- アカマイの配信系サービスを利用するにあたってゾーン頂点に CNAME を設定できない課題を解決
- トラフィック量に左右されない課金体系

Global Traffic Management
アカマイの配信技術に裏付けられた高機能なクラウド型 GSLB サービス

- 最大規模の DDoS に対してもパフォーマンスと可用性を継続的に確保できるように設計されたクラウド型 GSLB
- EDNS Client Subnet (ECS) を活用し、アカマイの配信を支えるインテリジェンスに基づく地理マッピング
- 負荷フィードバックに基づく高精度な加重負荷分散
- クラウドからの監視に基づく動的フェイルオーバー
- API によるリアルタイムな設定変更
- トラフィック量に左右されない課金体系

Shield NS53

オンプレの権威ネームサーバーを DDoS から保護するクラウド権威 DNS プロキシ

- GSLB 装置等アプライアンス型の権威ネームサーバーを利用している等といった理由で Edge DNS に移行できないユーザーに DDoS からの保護を提供
- IP エニーキャストで分散された豊富なキャパシティーをもつ拠点の DNS プロキシでキャッシュ、応答
- 水責め (PRSD、NXDOMAIN) 攻撃に対する保護機能
- GUI、API による柔軟な設定管理
- 顧客権威ネームサーバーに対するヘルスチェックとフェイルオーバー

あたらしかった dig

このプレゼンテーションにおいてなされる記述は作成者個人の見解を示すものであり、アカマイ・テクノロジーズの見解を示すものではありません。提供される情報は作成時点において正確なものであると考えておりますが、当該情報についてなんら表明又は保証を行いません。

DNS Summer Day 2023「あたらしい dig」おかげさまで好評でした

「あたらしい dig」の内容

- dig は DNS のふるまいを表現する標準語
- 思わぬ落とし穴
  - バージョンによって異なるデフォルト動作
  - ANY クエリーはデフォルトで TCP
- 知られざる便利なオプション
  - クエリも表示する +qr
- dig のオプションを整理

Qiita にふり返りの記事を書きました

https://qiita.com/ymatsumo/items/5a64cc19ebe432a05931

「チートシート、助かります！」

発表では分類しただけだったのですが… 作りました！

- A4 一枚 (PDF)に
- 簡単な説明
- デフォルト値

Qiita の記事で紹介しています。
「dig の全てのコマンドラインオプションを一覧にしたシートを作成しました」
https://qiita.com/ymatsumo/items/5a64cc19ebe432a05931

「+qr オプション、知りませんでした！」「+yaml オプション、知りませんでした！」

- yq というツールが便利
  https://github.com/mikefarah/yq
  YAML に対して jq と同じ操作ができる
  例) RCODE だけ取り出す

```
% dig +yaml example.com MX |yq
'.[].message.response_message_data.status'
NOERROR
%
```

  yq は XML や CSV にも対応

- +qr と +yaml を組み合わせると最強
  (+yaml は dig のバージョン 9.16～)

+yaml オプションの例

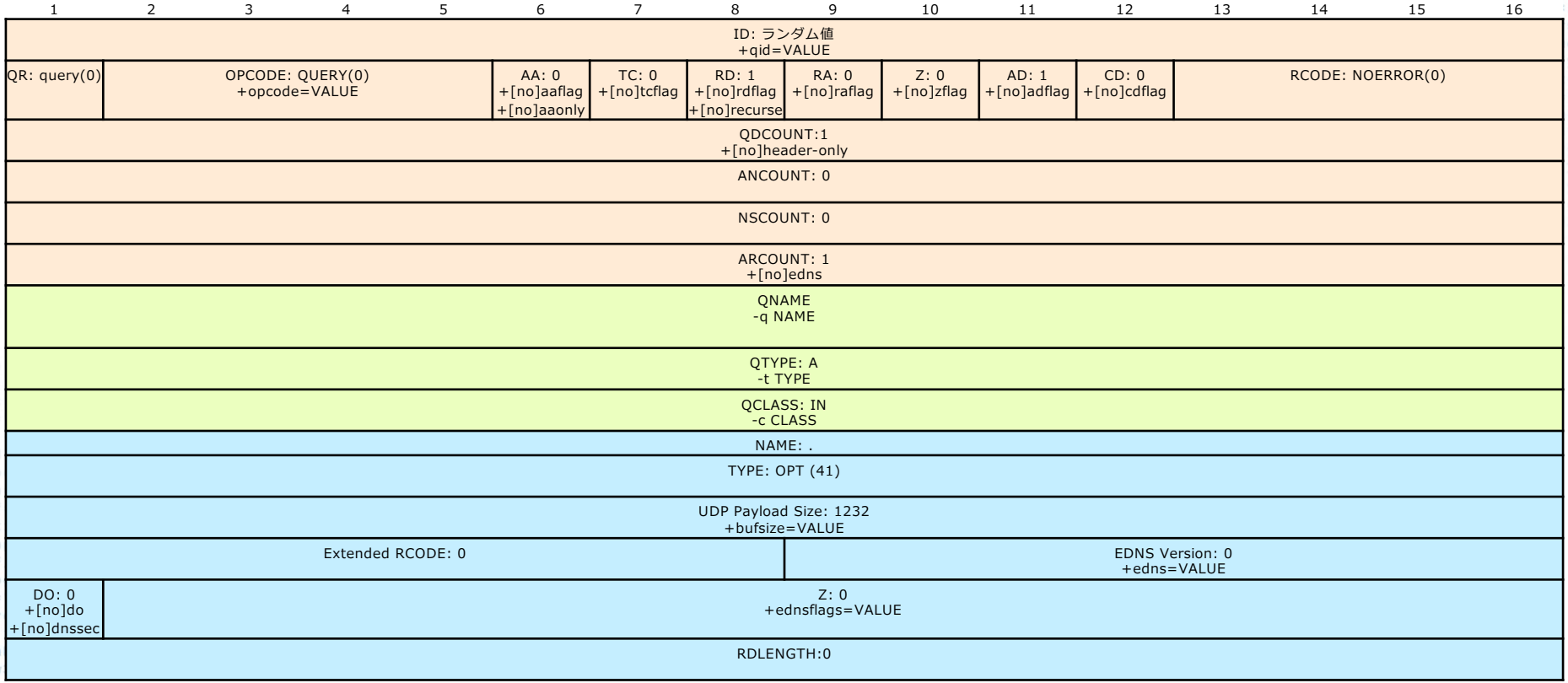
```
% dig +noedns +yaml example.com
-
  type: MESSAGE
  message:
    type: RECURSIVE_RESPONSE
    query_time: !!timestamp 2024-06-07T03:00:00.000Z
    response_time: !!timestamp 2024-06-07T03:00:00.006Z
    message_size: 45b
    socket_family: INET
    socket_protocol: UDP
    response_address: "203.0.113.1"
    response_port: 53
    query_address: "0.0.0.0"
    query_port: 0
    response_message_data:
      opcode: QUERY
      status: NOERROR
      id: 27491
      flags: qr rd ra ad
      QUESTION: 1
      ANSWER: 1
      AUTHORITY: 0
      ADDITIONAL: 0
      QUESTION_SECTION:
        - example.com. IN A
      ANSWER_SECTION:
        - example.com. 2316 IN A 192.0.2.1
%
```

kkey=value 形式で
人の目にもわかりやすい

「メッセージ・フォーマットとの対応が欲しい」

dig による DNS リクエストメッセージのデフォルト値と指定するためのコマンドラインオプション

※ EDNS オプションなし (+nocookie) の前提



「kdig 版ください！」

「kdig 版ください！」

(´･ω･`)しらんがな…でもざっくり比較

dig (9.19.24) と kdig (3.3.5) で比較

- 右に示したあたりはほぼ共通
- コメント表示部分を制御する
  +comments の効果が少し違い、
  +cmd のかわりに +header
- dig にしかないもの .. たくさん
- kdig にしかないもの .. 次ページ

-4
-6
@server
-p port
-b address
+[no]tcp
+[no]keepopen
+[no]https[=URL]
+[no]https-get
+[no]tls
+[no]tls-ca[=FILE]
+[no]tls-hostname=STR
+[no]tls-certfile=FILE
+[no]tls-keyfile=FILE
+[no]proxy=SADDR-DADDR
+[no]retry=N
+[no]timeout=T
+[no]ignore
+[no]badcookie
+[no]aaflag
+[no]tcflag
+[no]rdflag, +[no]recurse
+[no]raflag
+[no]zflag
+[no]adflag
+[no]cdflag
-q name / -t type / -c class
-k keyfile
-y [algo:]keyname:key

+[no]bufsize=B
+[no]edns[=N]
+[no]dnssec
+[no]nsid
+[no]subnet=SUBN
+[no]expire
+[no]cookie[=HEX]
+[no]padding[=N]
+[no]ednsopt=CODE[:HEX]
-x address
+[no]all
+[no]question
+[no]answer
+[no]authority
+[no]additional
+[no]stats
+[no]qr
+[no]ttl
+[no]class
+[no]crypto
+[no]generic
(+[no]unknownformat 相当)
+[no]multiline
+[no]short
+noidn
-V (-v 相当)
-h

dig にはなく kdig にあるコマンドラインオプション

- +[no]opt
- +[no]opttext
- +[no]optpresesnt
- +[no]tsig
- +[no]fastopen
- +[no]tls-pin=BASE64
- +[no]tls-sni=STR
- +[no]tls-ocsp-staping[=H]
- +[no]quic
- +[no]alignment[=N]
- +[no]json
- -d
- -E tapfile
- -G tapfile

- EDNS の表示に関する制御
- 暗号化周りのサポートが広い
- +fastopen も興味深い
- +json は (dig の +yaml と異なり)
  アンサーも構造化してくれる
- dnstap 形式 (tapfile) サポート
  -E 保存 -G 読み込み
- dig にはない +notsig があるのに +onesoa がない？

なお、kdig では NOTIFY でシリアルが指定できる


Akamai