dnsdist

DNSトラフィックに特化した
オープンソースの多機能ロードバランサー

DNS Summer Day 2019, Tokyo

2019-06-28

Open-Xchange プリセールスエンジニア
麻生 龍一 (ryuichi.aso@open-xchange.com)

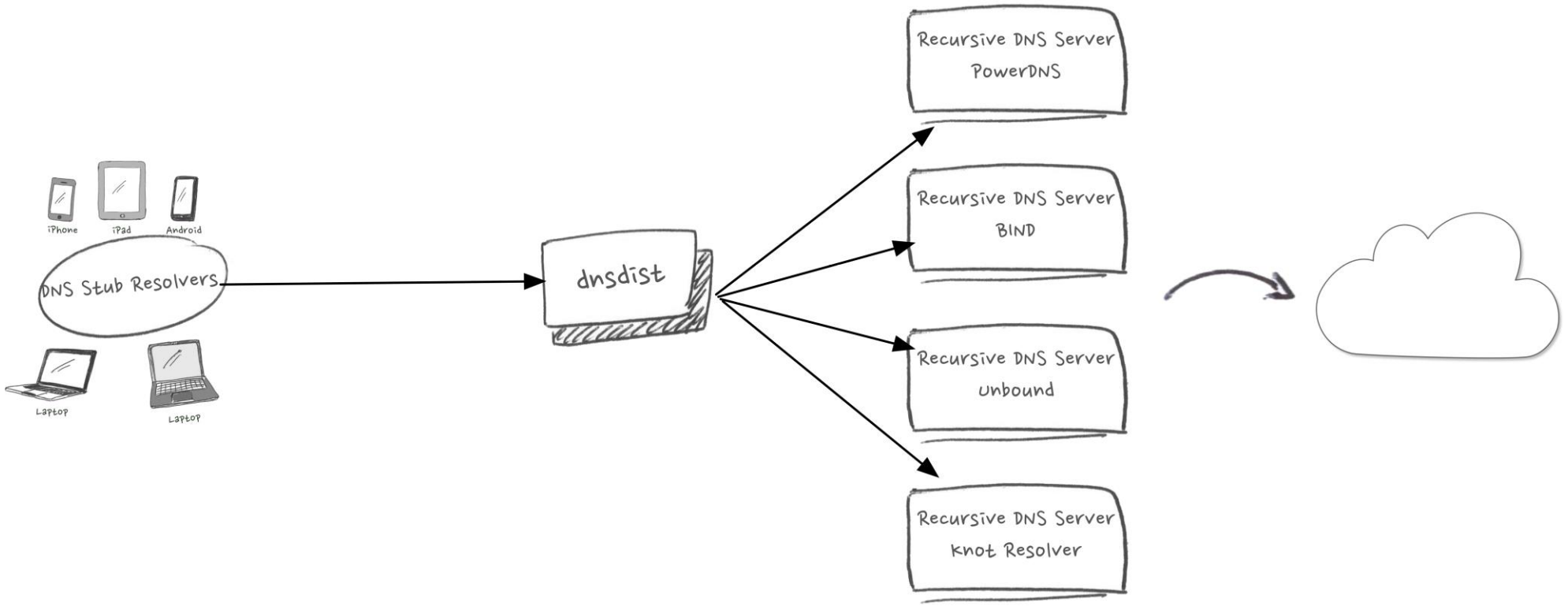
Stay Open.

dnsdistの概要

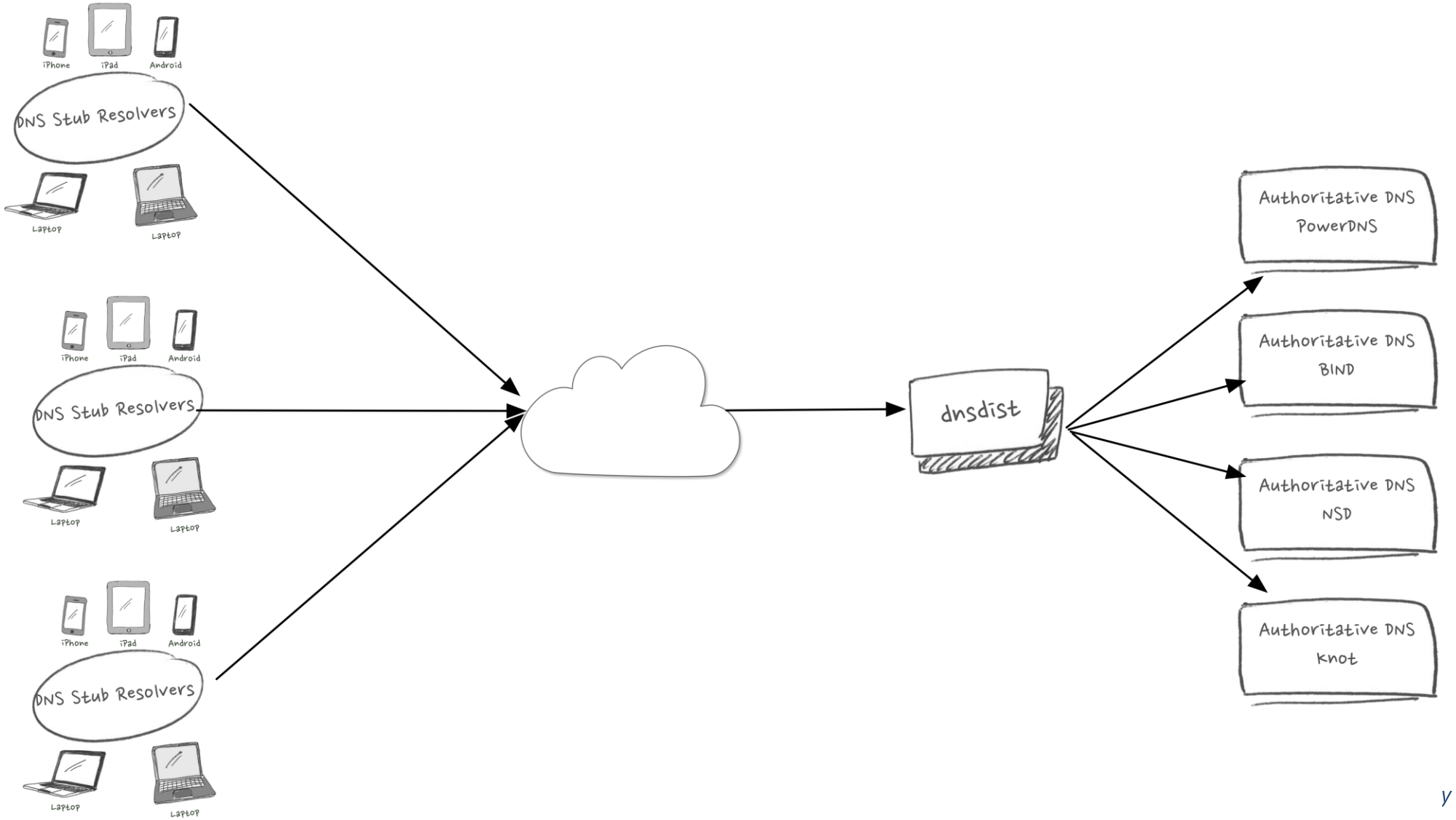
- DNSトラフィックに特化したロードバランサー
- PowerDNS.COM BV.が開発するオープンソース製品
- 多くのLinuxディストリビューションで動作
- Luaベースの柔軟な設定

dnsdistの概要

- バックエンドのDNSサーバーを選ばない



dnsdistの概要



インストールから起動まで

- リポジトリからのインストールが簡単（https://repo.powerdns.com）
- コマンドラインからの起動

  $ dnsdist -l 192.168.56.14:53 192.168.56.11 192.168.56.12

- 設定ファイル（/etc/dnsdist/dnsdist.conf）

  setLocal("192.168.56.14:53")
  newServer{address="192.168.56.11", qps=1000, weight=3, pool="recursor"}
  newServer{address="192.168.56.12", weight=1, pool="recursor"}
  newServer{address="192.168.56.11:5300", pool="auth"}

CLIとdnsdist

```
[root@centos614 ~]# dnsdist -c
> setServerPolicy(wrandom)
> showServerPolicy()
wrandom
>
> showServers()
#   Name Address              State Qps Qlim Ord Wt Queries Drops Drate  Lat Outstanding Pools
0        192.168.56.11:53        up 4.0 1000   1  3      75     0   0.0  3.3           0 recursor
1        192.168.56.12:53        up 1.0    0   1  1      26     0   0.0  6.3           0 recursor
2        192.168.56.11:5300      up 0.0    0   1  1       0     0   0.0  0.0           0 auth
All                                 3.0                101     0
> showBinds()
#   Address                       Protocol              Queries
0   0.0.0.0:53                    UDP                   101
1   0.0.0.0:53                    TCP                   0
>
```

dnsdistの機能

- DNSトラフィックを意識したロードバランシング
- 統計情報や問い合わせ履歴
- 条件を満たす問い合わせに対するアクション＝ルール
- Packet Cache
- DoT，DoHのエンドポイント

「スイス・アーミー・ナイフのような」多彩な機能

ロードバランシング

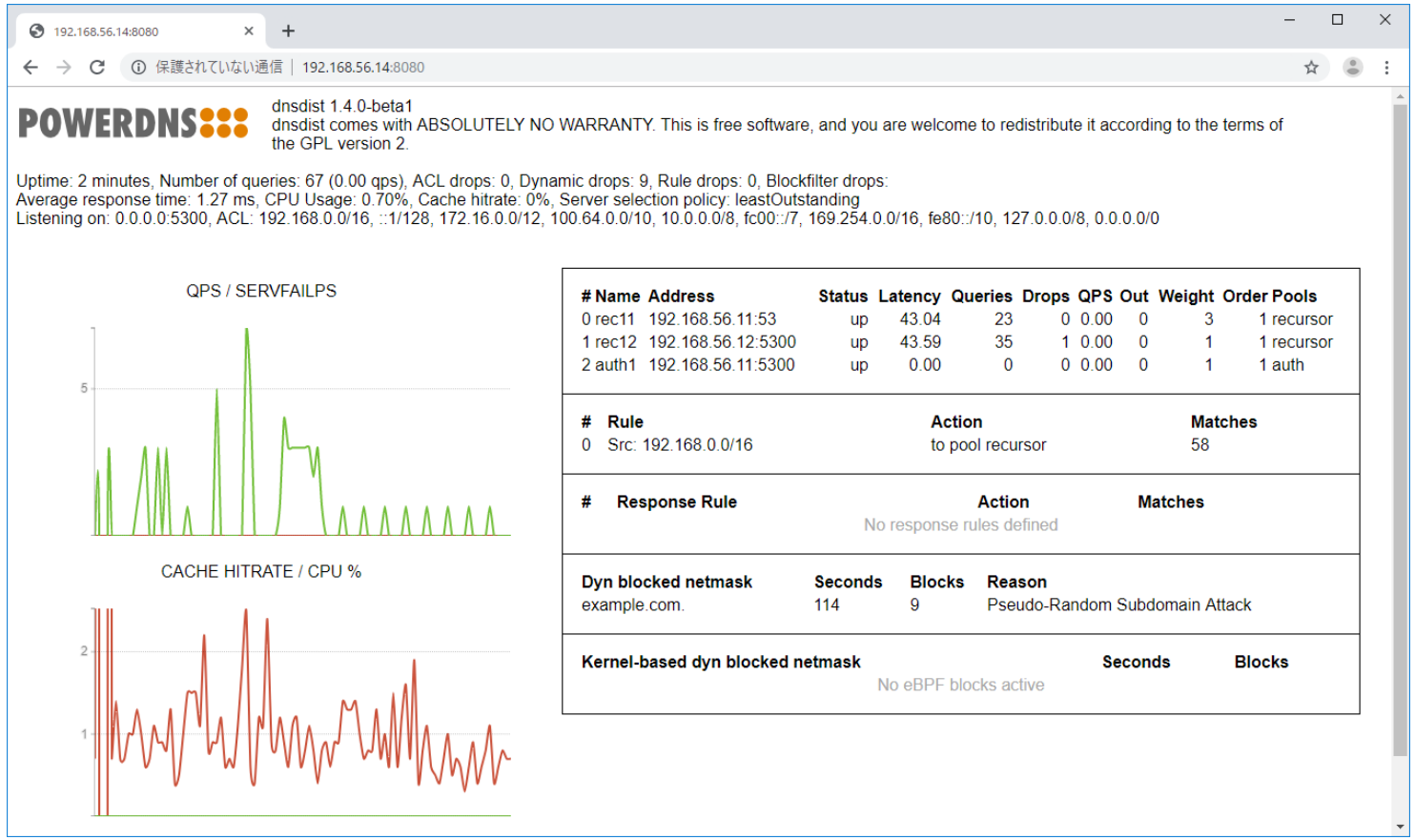
- DNSトラフィックを意識したロードバランシング
  - leastOutstanding（仕掛中の問い合わせが最も少ないサーバー）
  - firstAvailable（QPS上限以下で最初に見つかったサーバー）
  - wrandom（重み付きランダム）
  - roundrobin（ラウンドロビン）
  - whashed（重み付きハッシュ）
  - chashed（重み付きコンシステントハッシュ）
  - Luaによるカスタムポリシー

統計情報-問い合わせ履歴

```
[root@centos614 ~]# dnsdist -c
> topQueries(3)
   1  open-xchange.com.                        7 23.3%
   2  dsndist.org.                             4 13.3%
   3  www.powerdns.com.                        4 13.3%
   4  Rest                                    15 50.0%
>
> grepq('powerdns.com')
Time   Client                Server              ID    Name                Type Lat.  TC RD AA Rcode
-285.5 192.168.56.11:39156                       21180 www.powerdns.com.   A           RD    Question
-285.4 192.168.56.11:39156 192.168.56.11:53      21180 www.powerdns.com.   A    126.7  RD    No Error.
-126.3 192.168.56.11:35998                       27297 www.powerdns.com.   A           RD    Question
-126.0 192.168.56.11:35998 192.168.56.12:53      27297 www.powerdns.com.   A    288.5  RD    No Error.
-120.9 192.168.56.11:37341                       29585 www.powerdns.com.   A           RD    Question
-120.9 192.168.56.11:37341 192.168.56.11:53      29585 www.powerdns.com.   A    0.4    RD    No Error.
>
```

統計情報・問い合わせ履歴

- ビルトインWebサーバー



ルール＝セレクター＋アクション

セレクター	アクション
問い合わせ元IPアドレス 問い合わせパケット（QNAME，QTYPE，フラグ） ラベル数，QNAME長 応答メッセージ長，応答コード AND/OR/NOT，正規表現	特定のサーバープールに振り分け ドロップ，Rate Limit 各種応答（SERVFAIL, NXDOMAIN, REFUSED…） 応答を遅延 問い合わせ元IPアドレスをECSオプションに追加 フラグを除去

- ドメインや問い合わせ元IPアドレスに応じた設定

```
addAction({"example.com", "example.org"}, PoolAction("auth"))
addAction("192.168.0.0/16", PoolAction("recursor"))
addAction(AllRule(), RCodeAction(DNSRCode.REFUSED))
```

動的なルール生成

- 1秒おきに呼ばれるmaintenance関数内で評価→アクションを生成

```
function maintenance()
  addDynBlocks(exceedQRate(30, 10), "Exceeded query rate", 60, DNSAction.Refused)
  addDynBlocks(exceedQTypeRate(DNSQType.ANY, 5, 10), "Exceeded ANY rate", 60, DNSAction.Drop)
end
```

```
[root@centos614 ~]# dnsdist -c
> showDynBlocks()
What                  Seconds  Blocks Warning  Action           Reason
192.168.56.11/32           39       5 false    Send Refused     Exceeded query rate
>
```

DoT，DoHのエンドポイント

- DoT，DoHをサポートしていないDNSサーバーのフロントに配置
- 通常のDNSポートと変わらない設定

```
addLocal("192.168.56.12:53")
addTLSLocal("192.168.56.12:853", "/etc/dnsdist/server.crt", "/etc/dnsdist/server.key")
addDOHLocal("192.168.56.12:443", "/etc/dnsdist/server.crt", "/etc/dnsdist/server.key")
```

ぜひ使ってみてください

レポジトリ　https://repo.powerdns.com

公式サイト　https://dnsdist.org