DNSDIST

Um Balanceador e Canivete Suiço para DNS.

Quem sou.

Tech Lead no Mercado Livre.

15 anos em Network Datacenters e WebHosting.

Tio da Isa e da Manu.

Entusiasta de Automação.

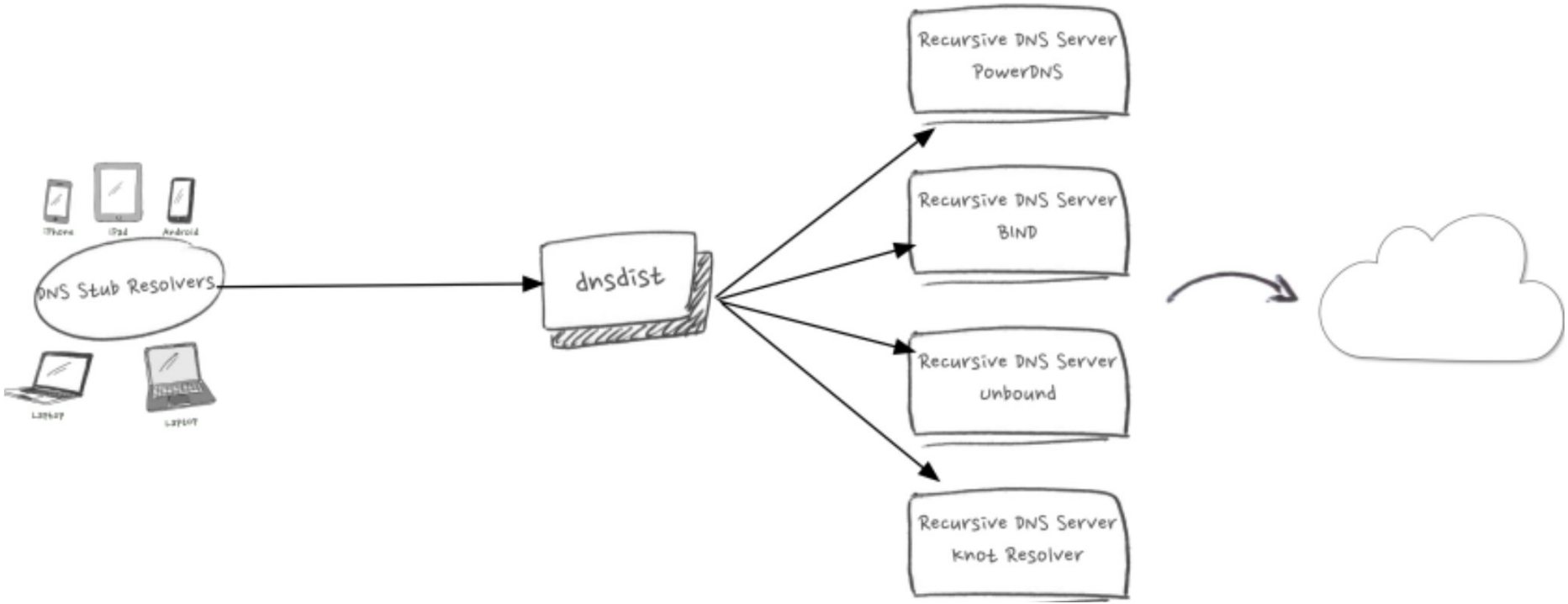
Porque falar de DNS ?

- Usualmente descartado como ofensor.
- É sempre o último a receber investimento.
- Diversas apresentações já abordaram os motivos de usar e cuidar de seu DNS recursivo.
- Porque mesmo falando e falando diversas vezes todos esquecem dele.

DNSDIST

- Escrito por Bert Hubert (PowerDNS).
- Criado para resolver problemas de Balanceamento do DNS.
- Primeira Apresentação na UKNOF34 e Aberto ao mundo na DNS-OARC 2015.
- Escrito em C++ e Lua 🇧🇷 (Snort, NMAP, WOL, Roblox).
- Rápido e Simples como tem que ser.

DNSDIST


DNS Stub Resolvers
dnsdist
Recursive DNS Server
PowerDNS
Recursive DNS Server
BIND
Recursive DNS Server
unbound
Recursive DNS Server
knot Resolver

DNSDIST

Uma Linha de Comando.

```
# dnsdist --local 0.0.0.0:53 192.168.1.2 127.0.0.1 192.168.1.79
```

e bem vindo DNSDIST.

```
> showServers()
#    Address                State     Qps    Qlim Ord Wt    Queries   Drops Drate   Lat
0    192.168.1.2:53            up  9999.7   10000   1  1     236655   46943  73.5   0.6
1    127.0.0.1:5300            up  5000.0    5000   2  1     106726    2476  25.5   1.2
2    192.168.1.79:5300         up  5034.0    7000   3  1      30954    4475 584.3  14.5
All                            20031.0                      374335   53894
```

DNSDIST

```
> topQueries(5)
   1  www.facebook.com.                      208  2.1%
   2  www.isg-apple.com.akadns.net.          198  2.0%
   3  FbCDn-PrOfiLE-A.akaMAihd.NeT.          194  1.9%
   4  www.google-analytics.com.              114  1.1%
   5  13.78.0.192.in-addr.arpa.               88  0.9%
   6  Rest                                  9198 92.0%
>
```

- showResponseLatency(): prints a histogram of response times
- showServers(): show statistics for all configured downstreams
- getServer(0):setDown(): force server 0 down administratively
- showPoolRules(): show configured pool rules
- showQPSLimiters(): show configured QPS limiters
- setServerPolicyLua(): configure Lua-based server policies

```
> showResponseLatency()
Average response latency: 0.582 msec
   msec
   0.10 .
   0.20 ****
   0.40 ************************************************************************
   0.80 ****
   1.60 .
   3.20
   6.40
  12.80
  25.60 *****
  51.20 ********
 102.40 *******
 204.80 *****
 409.60 ****
 819.20 *
1638.40 .
```

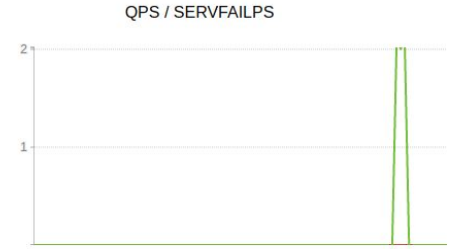
DNSDIST - WEB

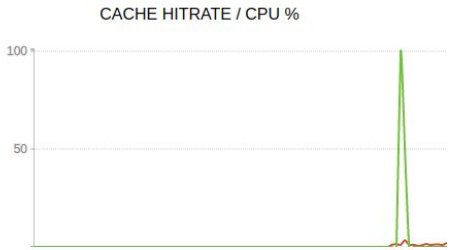
Interface Web com estatística de balanceamento e API.

POWERDNS

dnsdist 1.7.0
dnsdist comes with ABSOLUTELY NO WARRANTY. This is free software, and you are welcome to redistribute it according to the terms of the GPL version 2.

Uptime: 13 minutes, Number of queries: 355 (0.00 qps), ACL drops: 0, Dynamic drops: 0, Rule drops: 0
Average response time: 3.13 ms, CPU Usage: 2.10%, Cache hitrate: 0%, Server selection policy: leastOutstanding
Listening on: 0.0.0.0:53, ACL: 10.0.0.0/8, 100.64.0.0/10, 127.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.168.0.0/16, ::1/128, fc00::/7, fe80::/10





#	Name	Address	Status	Latency	Queries	Drops	QPS	Out	Weight	Order	Pools
0	1.1.1.1:853	1.1.1.1:853	up	27.30	48	0	0.00	0	1	1	
1	1.0.0.1:853	1.0.0.1:853	up	38.54	2	0	0.00	0	1	1	
2	1.1.1.1:443	1.1.1.1:443	up	17.11	73	0	0.00	0	1	1	
3	1.0.0.1:443	1.0.0.1:443	up	43.28	14	0	0.00	0	1	1	
4	9.9.9.9:853	9.9.9.9:853	up	15.67	19	0	0.00	0	1	1	
5	149.112.112.112:853	149.112.112.112:853	up	16.59	19	0	0.00	0	1	1	
6	9.9.9.9:443	9.9.9.9:443	up	21.73	20	0	0.00	0	1	1	
7	9.9.9.9:5053	9.9.9.9:5053	up	21.66	10	0	0.00	0	1	1	
8	149.112.112.112:443	149.112.112.112:443	up	16.86	24	0	0.10	0	1	1	
9	149.112.112.112:5053	149.112.112.112:5053	up	17.42	17	0	0.00	0	1	1	

#	Rule	Action	Matches
No rules defined			

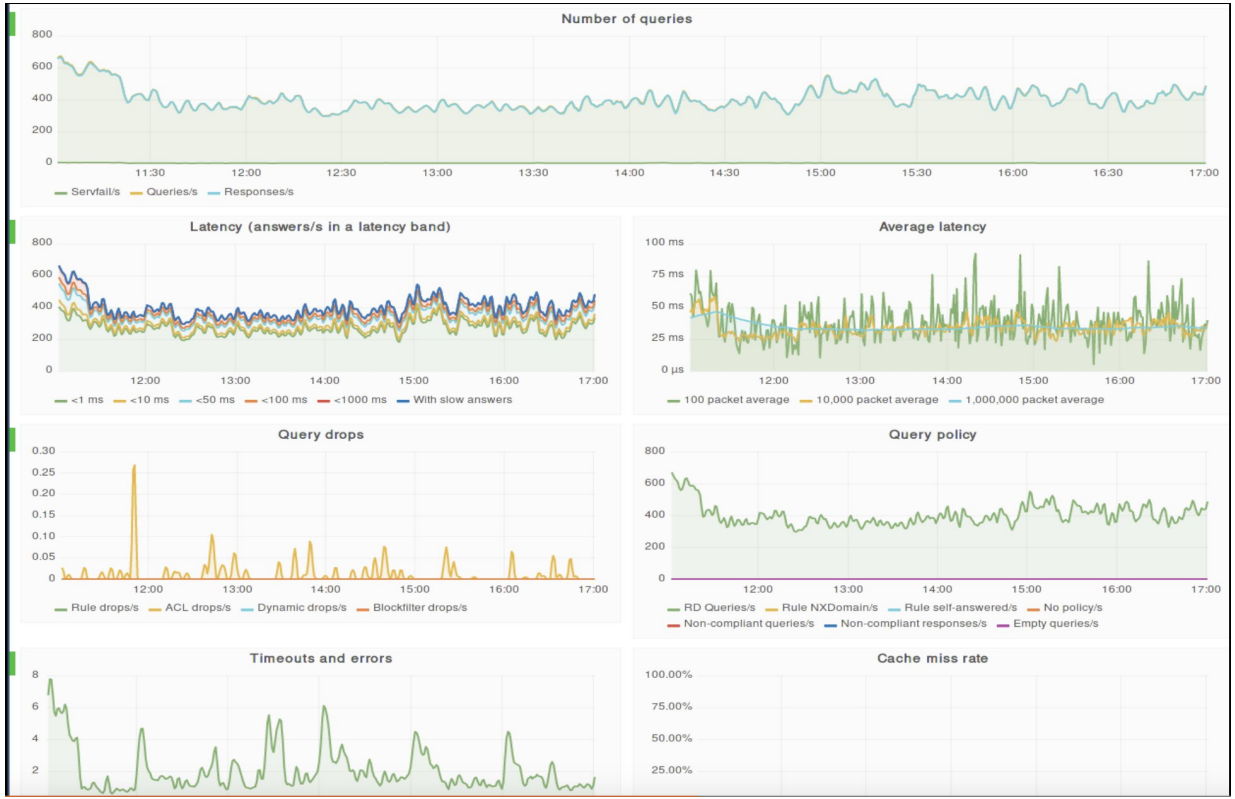
#	Response Rule	Action	Matches
No response rules defined			

Dyn blocked netmask	Seconds	Blocks	Reason
No dynamic blocks active			

Kernel-based dyn blocked netmask	Seconds	Blocks
No eBPF blocks active		

DNSDIST - Telemetria

Envio de Telemetria baseado no protocolo Carbon.



DNSDIST - CLI

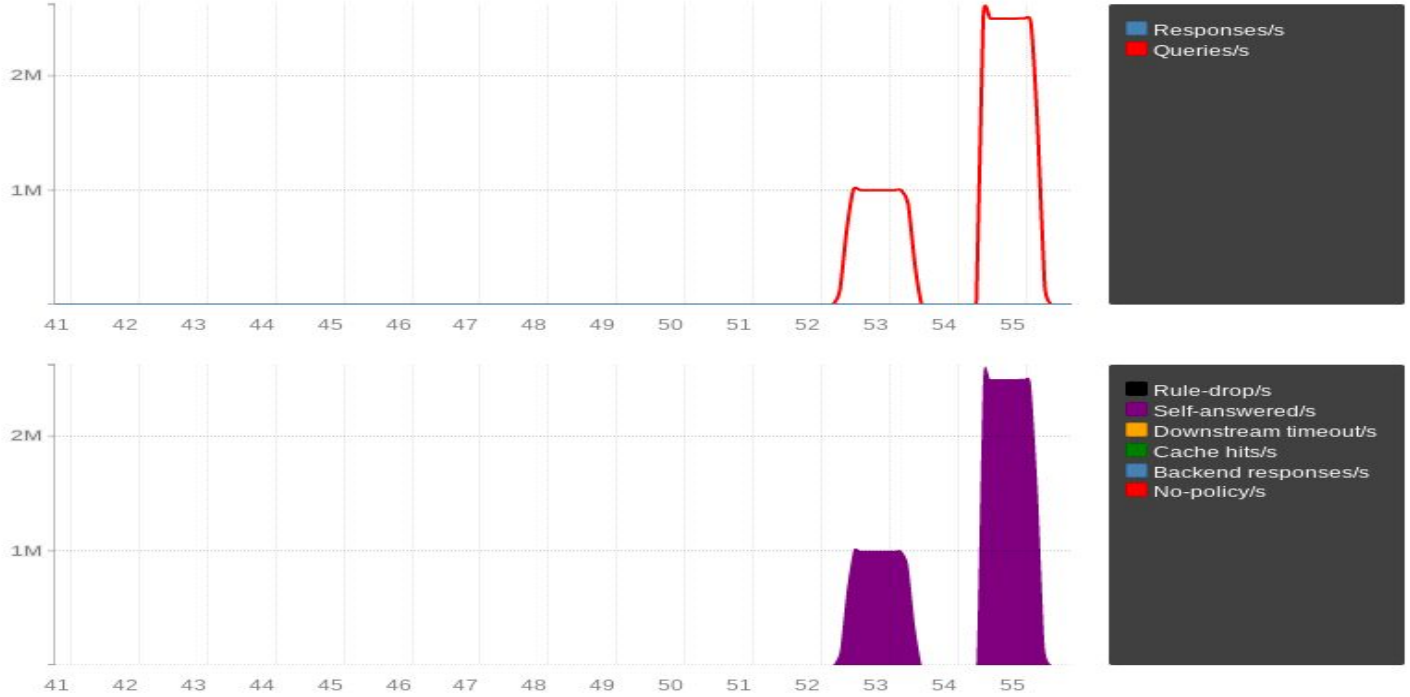
Por meio do CLI é possível usar GREP para encontrar domínios que estão passando pelo DNSDIST.

```
> grepq('ru', 2)
Time  Client              Server          ID    Name         Type Lat. TC RD AA Rcode
-0.2  192.0.2.92:33846                    4905  hehehey.ru.  ANY          RD    Question
-0.2  192.0.2.92:33846    127.0.0.1:5300 4905  hehehey.ru.  ANY  0.2     RD    Non-Existent domain
-0.2  192.0.2.92:33846                    4907  hehehey.ru.  ANY          RD    Question
-0.2  192.0.2.92:33846    127.0.0.1:5300 4907  hehehey.ru.  ANY  0.3     RD    Non-Existent domain

> grepq({'apple.com.', "100ms"}, 5)
Time    Client              Server          ID    Name           Type Lat.  TC RD AA Rcode
-127.6  192.0.2.92:43583    127.0.0.1:5300 44987 cl4.apple.com. A    247.2    RD    No Error. 4 answers
```

DNSDIST - Performance

Via AF_XDP / XSK é possível escalar um único balancer para 2.5M de Query por segundo.



DNSDIST

- Adição de informação nas query (Flags, EDNS Client Subnet).
- Roteamento a Pools específicos para Abuse.
- Roteamento a Pools específicos para DNSSEC.
- Drop Query.
- Delay Query.
- Detecção e Mitigação de DOS com EBPF.
- Mecanismo de Transição para DNS IPV6/IPV4.
- Cache HOT.
- Pode ser combinado com Anycast.

Referências

https://media.frnog.org/FRnOG_28/FRnOG_28-5.pdf

https://dnsdist.org/

https://berthub.eu/articles/posts/history-of-powerdns-2013-2020/

https://blog.powerdns.com/

https://blog.powerdns.com/improving-dnsdist-performance-with-af_xdp

Dúvidas ?