



IX – FORUM REGIONAL - SP

Dns de alta disponibilidade usando UNBOUND + QUAGGA + ECMP

GIOVANELI
CONSULTORIA E TREINAMENTOS



Quagga + UNBOUND + ECMP

Solução de alta disponibilidade para cargas
Extremas em DNS Recursivo.

- Alexandre Giovaneli – Giovaneli Consultoria



Quagga + UNBOUND + ECMP

- Objetivo da solução
 - Visto que nos últimos anos os provedores de internet tiveram um crescimento exponencial e os alto custo para servidores DNS recursivo , nos fez buscar uma solução totalmente “OPEN-SOURCE” para atender estes provedores de internet de 3 mil usuários até 50 mil usuários.
 - Esta solução foi implementada inicialmente em alguns provedores como beta, e nos surpreendeu muito o resultado satisfatório.
 - Totalmente compatível com IPv4 & IPv6



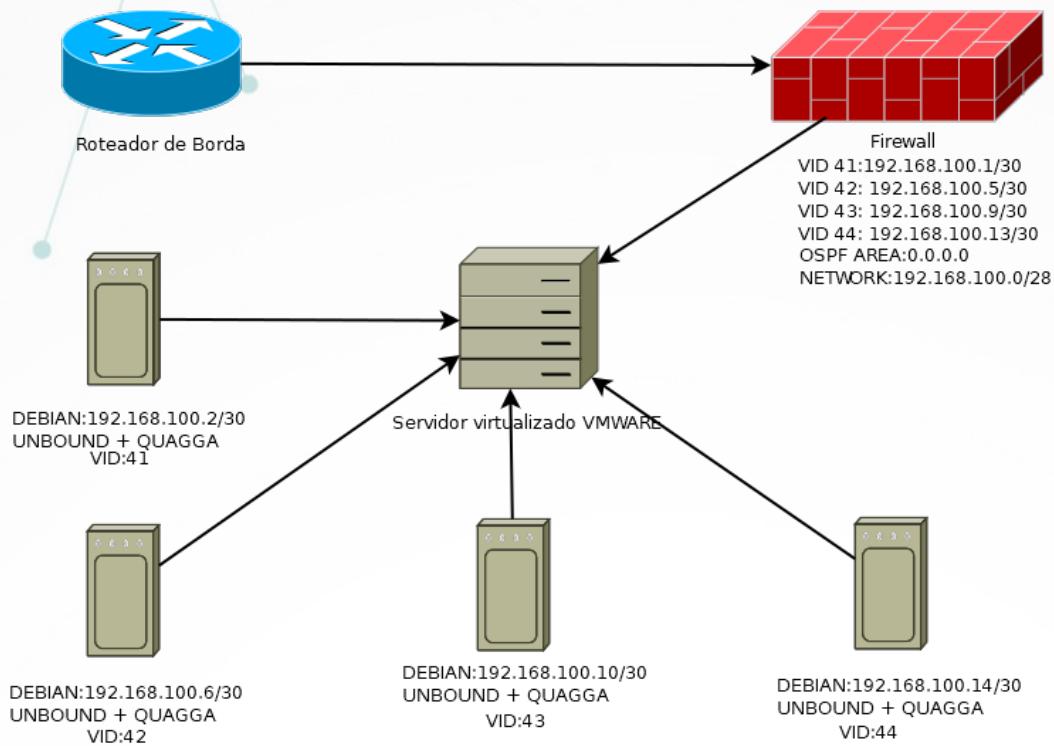
Quagga + UNBOUND + ECMP

- Vantagens de se ter um DNS Local anycast
 - Melhor tempo de resposta nas consultas
 - Maior resiliência do serviço de DNS
 - Compatibilidade 100% com CGNAT não é necessário ter uma regra de NAT até chegar ao DNS.
 - Melhor fluidez do tráfego na rede
 -



Quagga + UNBOUND + ECMP

- Como funciona a solução:
 - A solução é compilada usando dois Daemons em Debian sendo:
 - Quagga
 - Unbound
 - O Gateway deste DNS deverá ter obrigatoriamente suporte a ECMP (Equal Cost Multi Path)
 - O ECMP fará o papel de balancear a carga entre duas rotas iguais, neste cenário usamos os seguintes endereços ips:
 - 10.1.1.1
 - 10.2.2.2



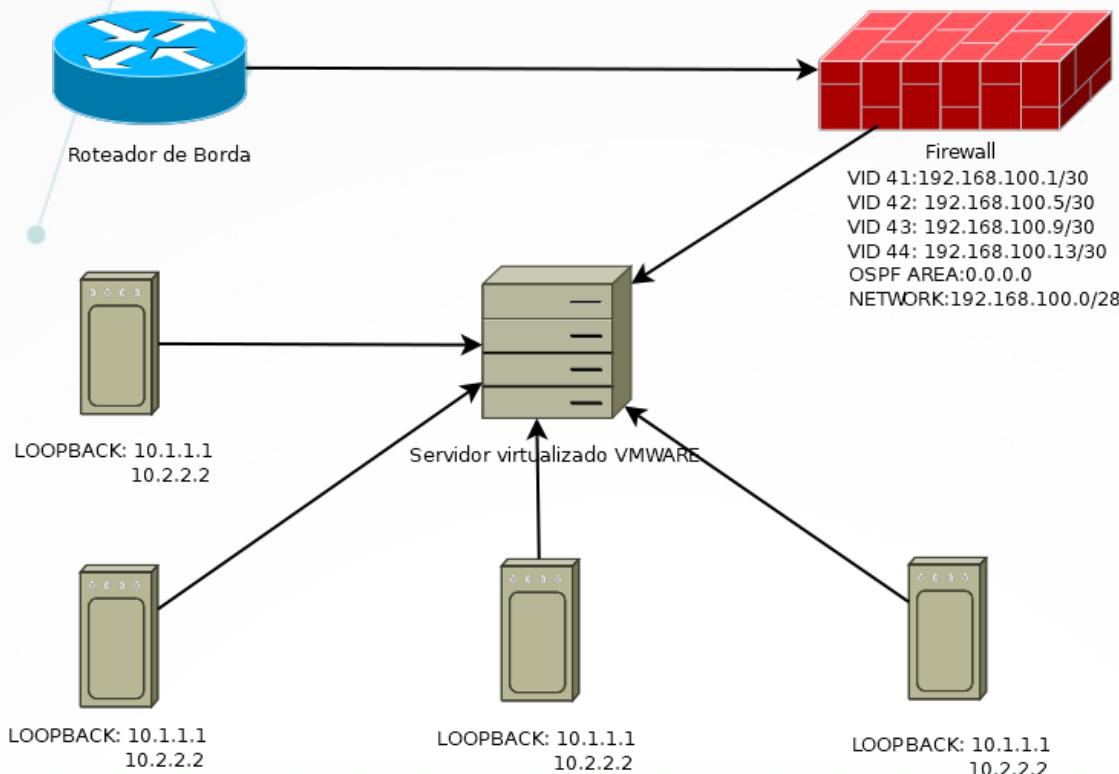


Quagga + UNBOUND + ECMP

- Como funciona o anycast
 - Qualquer pacote enviado para o ip 10.1.1.1 ou 10.2.2.2 o ECMP no firewall rodando OSPF irá enviar para um dos servidores dns onde neste cenário ele terá na tabela de rotas 4 rotas instaladas sendo:
 - DST:10.1.1.1 > GW:192.168.100.2
 - DST:10.1.1.1 > GW:192.168.100.6
 - DST:10.1.1.1 > GW:192.168.100.10
 - DST:10.1.1.1 > GW:192.168.100.14



Quagga + UNBOUND + ECMP





Quagga + UNBOUND + ECMP

- Instalando Quagga e unbound (lembre de estar no modo sudo , digite su e entre com a senha de root)
 - apt-get install quagga
 - apt-get install unbound
- Após a instalação edite o arquivo daemon do quagga
 - nano *etc/quagga/daemon*
 - *Nas linhas ospfd e zebra coloque na frente “yes” e save as configurações*
 - *zebra = yes*
 - *ospfd = yes*



Quagga + UNBOUND + ECMP

- Digite os seguintes comando no modo sudo
 - cp /usr/share/doc/quagga/examples/zebra.conf.sample /etc/quagga/zebra.conf
 - cp /usr/share/doc/quagga/examples/ospfd.conf.sample /etc/quagga/ospfd.conf
- chown quagga.quaggavty /etc/quagga/*.conf
- chmod 640 /etc/quagga/*.conf
- service quagga restart



Quagga + UNBOUND + ECMP

- Configurando ospf e logando no quagga:
 - telnet localhost 2604
 - Entre com a senha paadrão: zebra
 - Entre com a senha padrao : en
 - conf t
 - router ospf
 - network 192.168.100.0/28area 0
 - router-id 177.66.247.25
 - redistribute static
 - redistribute connected
 - redistribute kernel
 - Wr
 - exit
- Configurando ips de loopback:
 - telnet localhost 2601
 - zebra
 - en
 - zebra
 - conf t
 -
 - interface lo
 - ip address 10.1.1.1/32
 - ip address 10.2.2.2/32
 -
 - exit
 - wr
 -



Quagga + UNBOUND + ECMP



- Configurando unbound e comentando os itens mais importantes para a instalação:

- `nano /etc/unbound/unbound.conf`
server:
port: 53

Interface: 10.1.1.1 # aceita requisições neste ip de loopack

Interface: 10.2.2.2 # aceita requisições neste ip de loopack

Interface: 127.0.0.1 # aceita requisições neste ip de loopack

access-control: 0.0.0.0/0 refuse # negando redes externas

access-control: 127.0.0.0/8 allow #aceita que esta sub-rede consulte o dns

access-control: 192.168.0.0/16 allow #aceita que esta sub-rede consulte o dns

access-control: 172.16.0.0/12 allow #aceita que esta sub-rede consulte o dns

access-control: 100.64.0.0/10 allow #aceita que esta sub-rede consulte o dns

access-control: 10.0.0.0/8 allow #aceita que esta sub-rede consulte o dns



Quagga + UNBOUND + ECMP

- Configurando unbound e comentando os itens mais importantes para a instalação:

- nano *etc/unbound/unbound.conf*
server:
port: 53

Interface: 10.1.1.1 # aceita requisições neste ip de loopack

Interface: 10.2.2.2 # aceita requisições neste ip de loopack

Interface: 127.0.0.1 # aceita requisições neste ip de loopack

access-control: 0.0.0.0/0 refuse # negando redes externas

access-control: 127.0.0.0/8 allow #aceita que esta sub-rede consulte o dns

access-control: 192.168.0.0/16 allow #aceita que esta sub-rede consulte o dns

access-control: 172.16.0.0/12 allow #aceita que esta sub-rede consulte o dns

access-control: 100.64.0.0/10 allow #aceita que esta sub-rede consulte o dns

access-control: 10.0.0.0/8 allow #aceita que esta sub-rede consulte o dns





Quagga + UNBOUND + ECMP



- Atualmente todos os roteadores de mercado suportam **ECMP (multip-path)**:
 - Mikrotik (já vem de fábrica configurado)
 - Juniper é necessário configurar

```
[edit]
root@vMX-1# set routing-options forwarding-table export load-balance

[edit]
root@vMX-1# set policy-options policy-statement load-balance then load-balance per-packet
```

- Cisco: Vem configurado por padrão
- Huawei: Vem configurado por padrão
- Datacom: É necessário configurar o multi-path
- Vyos : Vem de fábrica configurado



Quagga + UNBOUND + ECMP



- Após a configuração
 - service unbound restart
 - Dica 1: caso der algum erro no reload confira se existe caracteres a mais ou se segue o padrão de configuração demonstrado.
 - Dica 2: Confira se o ip de loopback colocado está configurado previamente no zebra ou nas interfaces .
 - Coloque um /30 valido par cada servidor, a consulta aos root server usará este ip valido, porem o ip da consulta pode ser invalido.



Quagga + UNBOUND + ECMP



GIOVANELI
CONSULTORIA E TREINAMENTOS





Quagga + UNBOUND + ECMP



- Para checar se as requisições estao chegando instale o tcpdump:
 - apt-get install tcpdump
 - tcpdump udp port 53 -n
- Ao ver os tcpdump nas 4 maquinas você ira perceber que os 4 estão respondendo requisições na mesma quantidade



Quagga + UNBOUND + ECMP

- Dicas de uso do DNS anycast:
 - Para uma rápida migração do serviço de DNS você pode adicionar os ips dos DNS atuais na loopback dentro do qagga e adicionar as interfaces dentro do unbound para “escutar” as requisições de DNS neste novo ip.
- Sequestro de servidores DNS de maliciosos
 - Você “pode” adicionar por exemplo um servidor DNS que esteja configurando nos roteadores para abusos e phishing.



Quagga + UNBOUND + ECMP

- Dicas de uso do DNS anycast:
 - Para uma rápida migração do serviço de DNS você pode adicionar os ips dos DNS atuais na loopback dentro do qagga e adicionar as interfaces dentro do unbound para “escutar” as requisições de DNS neste novo ip.
- Sequestro de servidores DNS de maliciosos
 - Você “pode” adicionar por exemplo um servidor DNS que esteja configurando nos roteadores para abusos e phishing.

- Muito obrigado a todos



Alexandre Giovaneli
CEO
📞 +55 31 9 8255-5555
noc@giovaneli.net
www.giovaneli.net

