DNS ANYCAST

O QUE NÃO TE CONTARAM POR TRÁS DO NOME BONITO

GTER 51 | 2022
SÃO PAULO

NEXTHOP SOLUTIONS

NETWORK EDUCATION

APRESENTAÇÃO

GTER 51 | 2022
SÃO PAULO

Me chamo Elizandro Pacheco e atuo com provedores regionais desde os anos 2000.

Fundador da NextHop Solutions ®, empresa especializada em soluções para provedores de acesso.

Fundador da Network Education ®, empresa especializada em treinamentos para profissionais que atuam na área de redes.

Autor do Livro Docker para Provedores.

Palestrante nos maiores e melhores eventos do ramo por todo Brasil.

GTER 51 | 2022
SÃO PAULO

O BÁSICO SOBRE DNS RECURSIVO

O QUE VOCÊ NÃO DEVE DEIXAR DE SABER

Checklist de DNS Recursivo

- NUNCA USE DNS DE TERCEIROS
- Escolha o software que você mais domina! Tanto o bind quanto o unbound são bons softwares.
- Jamais coloque seu DNS atrás de um NAT.
- Dimensione corretamente o seu hardware e ajuste sua configuração para ele.
- Monitore
- Não seja permissivo nas suas ACLs e Firewall
- Não tenha apenas um, se você domina o sistema, USE ANYCAST.
- **Mikrotik/RouterOS NÃO É UM SERVIDOR RECURSIVO COMPLETO.**

GTER 51 | 2022
SÃO PAULO

NEXTHOP SOLUTIONS

NETWORK EDUCATION

GTER 51 | 2022
SÃO PAULO

ANYCAST E ROTEAMENTO

COMO FUNCIONA

O QUE É O ANYCAST

Anycast, basicamente é um método de endereçamento e roteamento de rede que te permite rotear "solicitações" para dispositivos diferentes.

- É uma comunicação de "um pra um de muitos".
- Através do protocolo de roteamento permite que diversos dispositivos "escutem" o(s) mesmo(s) endereço(s) IP.
- Como resultado você tem diversos dispositivos com o "mesmo endereçamento" e o que responde as solicitações é o que está "mais perto topologicamente", daquele que originou a requisição.

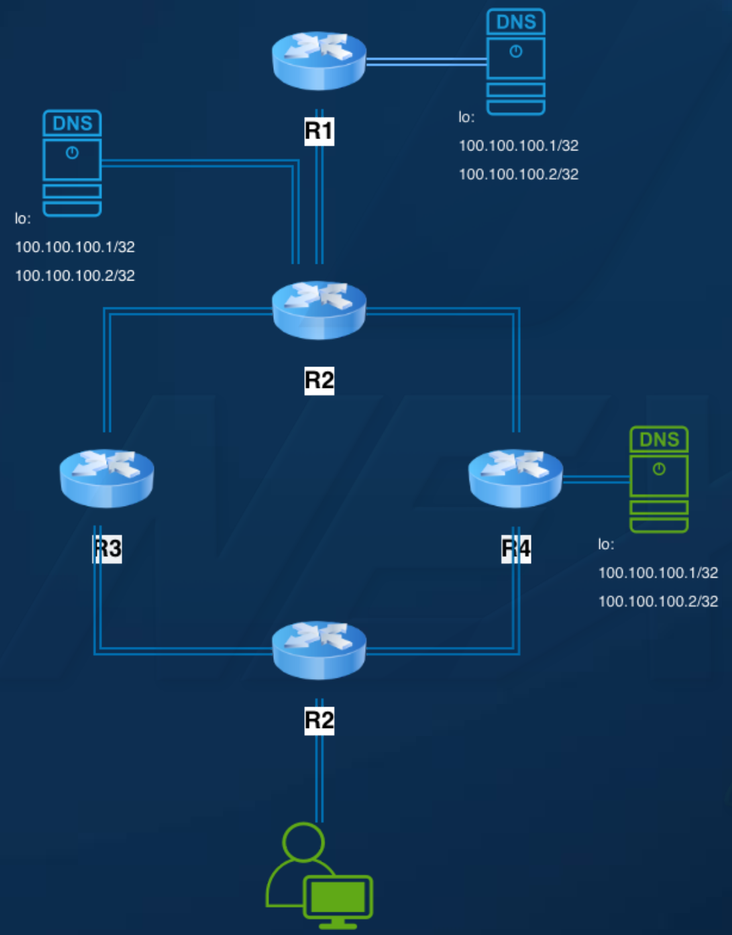
GTER 51 | 2022
SÃO PAULO

VANTAGENS DO ANYCAST

Em um ambiente onde você utiliza anycast para seus servidores DNS você garante diversas vantagens sobre a forma tradicional de se fazer dns.

Dentre elas destaco:

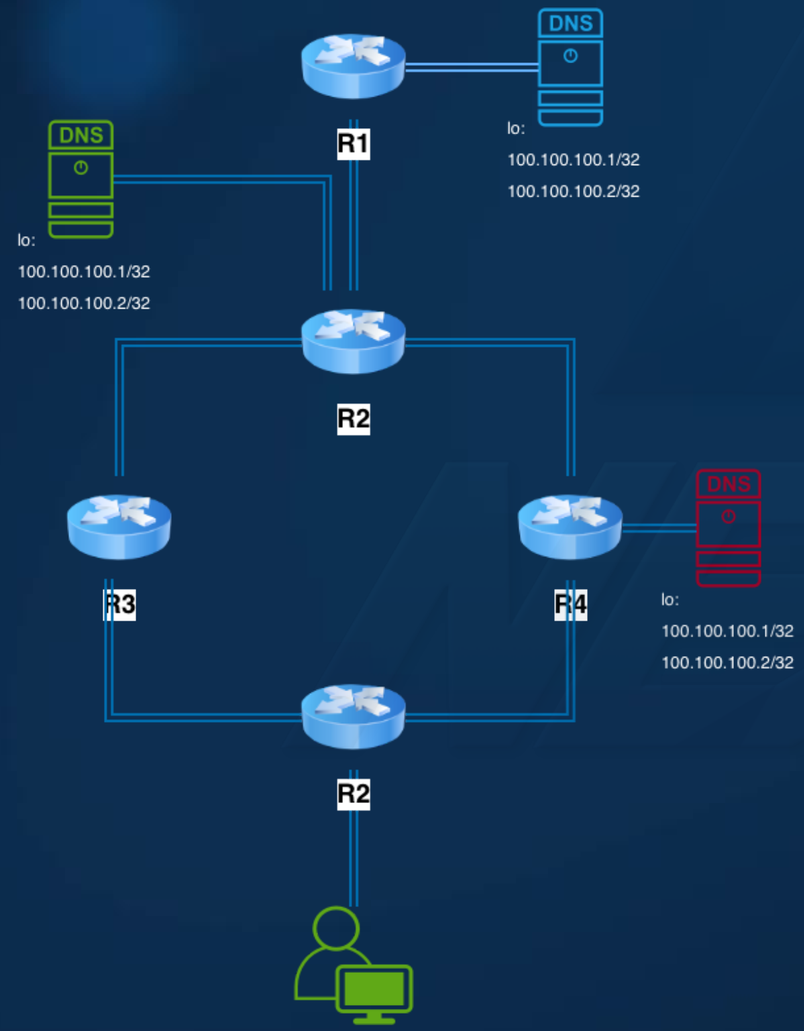
- Alta Disponibilidade
- Escalabilidade
- Divisão de carga igualitária



GTER 51 | 2022
SÃO PAULO

VANTAGENS DO ANYCAST

Em caso de falha do servidor mais próximo, o segundo mais próximo atende.

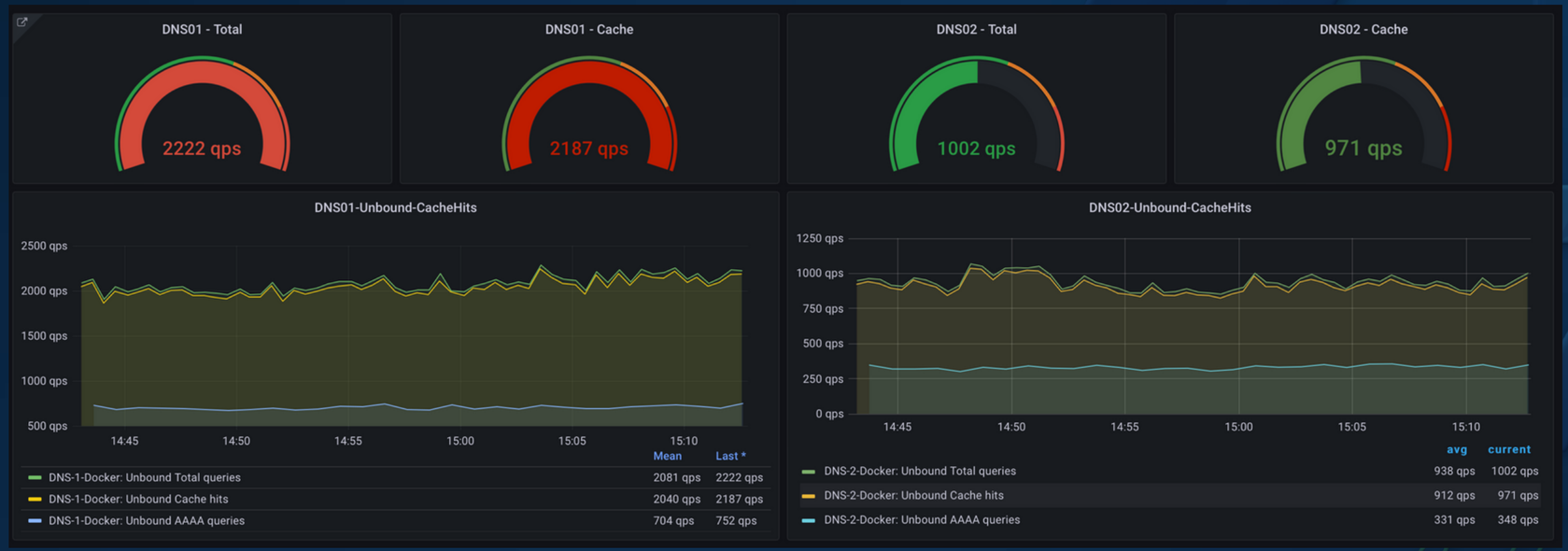


GTER 51 | 2022
SÃO PAULO

ROTEAMENTO E ECMP

Em geral, quando você utiliza 2 servidores recursivos na sua rede, notará que o "primário" sempre terá mais requisições que o secundário.

Isso acontece devido a forma que os sistemas operacionais lidam com as requisições DNS.



GTER 51 | 2022
SÃO PAULO

ROTEAMENTO E ECMP

Com anycast você poderá desfrutar ainda do ECMP (Equal-Cost Multi-Path).

ECMP é um método de roteamento de múltiplos caminhos que nos permite fazer o balanceamento de carga/tráfego.

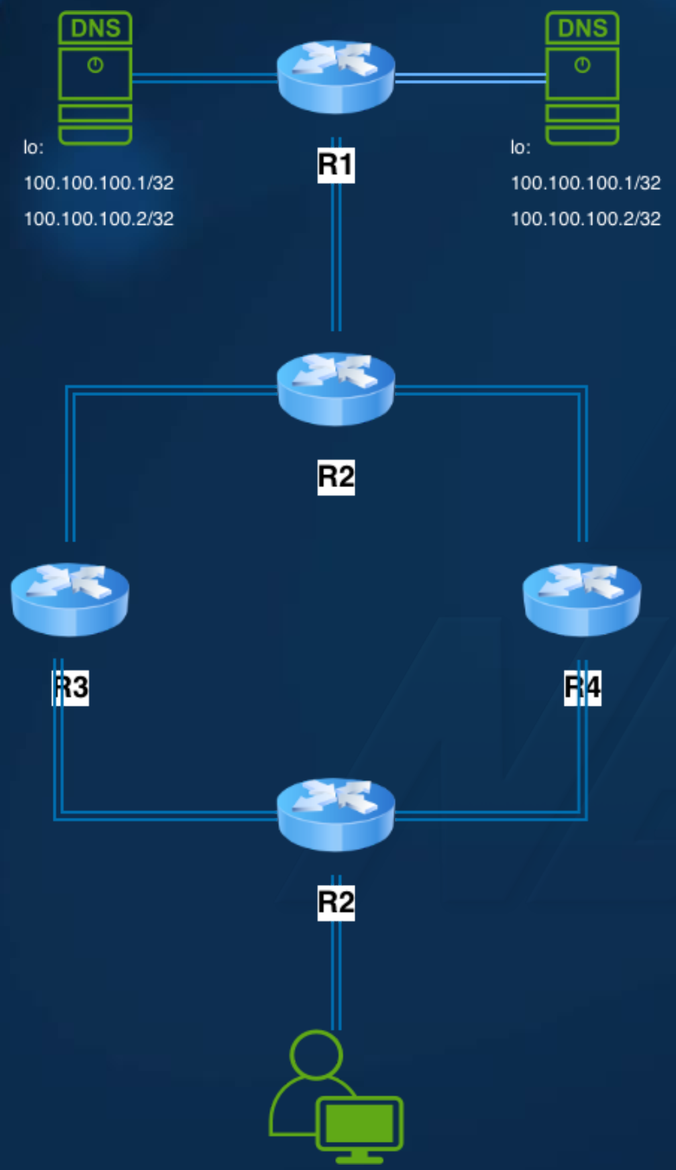
De forma resumida, quando duas rotas "empatam", o tráfego é dividido entre elas.

Junte isso ao anycast, e você além de prover alta disponibilidade e redundância eficientes, terá uma divisão plena de carga entre os seus servidores.

Basta projetá-los de forma que, topologicamente, esse "empate" aconteça.

GTER 51 | 2022
SÃO PAULO

ROTEAMENTO E ECMP



GTER 51 | 2022
SÃO PAULO

O QUE É NECESSÁRIO?

- Software que "transforme" seu servidor linux em um "roteador" (FRR é uma ótima opção).
- Definição do protocolo (BGP ou OSPF) a ser utilizado.
- Configuração da vizinhança com sua rede no protocolo escolhido.
- Adição dos endereços (que responderão no recursivo) na loopback.
- Anúncio/Configuração da utilização desses endereços pelos clientes.
- Além, claro, da configuração do serviço de dns no daemon escolhido.

GTER 51 | 2022
SÃO PAULO

FRR (https://frrouting.org)

Em uma instalação limpa do Debian 11, basta instalar via apt:

$ apt install frr

Outros métodos de instalação podem ser encontrados na documentação oficial do projeto:

http://docs.frrouting.org/en/latest/index.html

GTER 51 | 2022
SÃO PAULO

FRR (https://frrouting.org)

A partir deste ponto, você deve escolher o protocolo, estabelecer as vizinhanças e configurar o serviço em sí.

Recomendação de bons tutoriais:

Marcelo Gondim
https://wiki.brasilpeeringforum.org/w/DNS_Recursivo_Anycast_Hyperlocal

Rudimar Remontti
https://blog.remontti.com.br/4771

GTER 51 | 2022
SÃO PAULO

GTER 51 | 2022
SÃO PAULO

PONTOS DE ATENÇÃO

O QUE NÃO TE CONTARAM
(OU VOCÊ NÃO VIU)

NAT

Sim, parece repetitivo (e ainda vou falar novamente dele) mas o NAT é um dos maiores pontos de atenção!

Não raramente encontramos servidores atrás de NAT e o resultado disso pode ser catastrófico pra sua rede.

Geralmente por situações assim é que surgem as falácias de "o do google é o melhor do melhor do mundo", "já tive dns interno e só me incomodei", e tantas outras bobagens que ouvimos por aí.

Entenda que: Principalmente se você estiver utilizando anycast, você exportará endereços que seu serviço deve escutar para a sua rede, MAS NÃO DEVE UTILIZAR ESSE ENDEREÇO PARA COMUNICAÇÃO DA MÁQUINA.

E, ainda que você use IPs privados no serviço, para conectividade da máquina à internet UTILIZE UM PÚBLICO.

Enderece corretamente o Unbound

O Unbound possui configurações específicas tanto para em qual endereço ele deve "ouvir" tanto quanto para endereços que ele deve "usar para conexão com a internet".

O parâmetro **interface** diz respeito à quais endereços o serviço vai "ouvir".

Nele, coloque os prefixos IPV4 E IPV6 que devem responder as requisições.

interface: 127.0.0.1
interface: 100.100.100.100/32
interface: 100.100.100.101/32
interface: 2001:db8::100/32
interface: 2001:db8::101/32

NÃO USE 0.0.0.0 E ::0

GTER 51 | 2022
SÃO PAULO

Enderece corretamente o Unbound

Atente-se ao parâmetro **outgoing-interface** pois ele é quem indica quais endereços serão usados pelo servidor para realizar as requisições externas (saída para a internet).

```
outgoing-interface: IPV4-PÚBLICO
outgoing-interface: IPV6-GLOBAL
```

E claro, apesar de um servidor IPv4 ser capaz de dar respostas sobre endereços IPv6, o IDEAL é que ele seja capaz de aceitar as requisições nativamente em ambos protocolos:

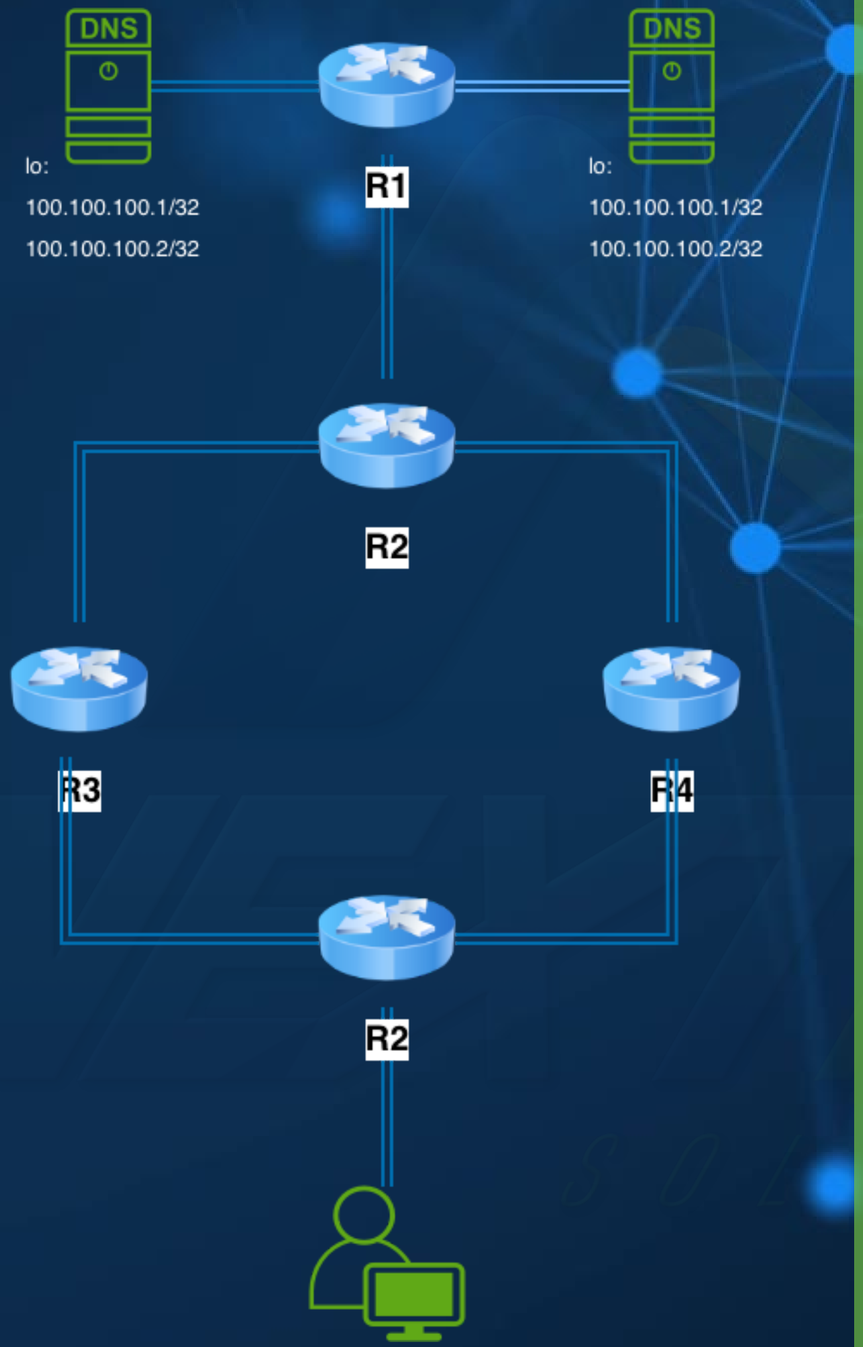
```
do-ip4: yes
do-ip6: yes
do-udp: yes
do-tcp: yes
```

Monitore

Quando você utiliza anycast você deve redobrar a atenção ao monitoramento.

Imagine, no cenário ao lado, **que o serviço** do unbound parou mas a máquina (e o frr) continuaram funcionando...

Quais sintomas você pode enfrentar?



GTER 51 | 2022
SÃO PAULO

Monitore

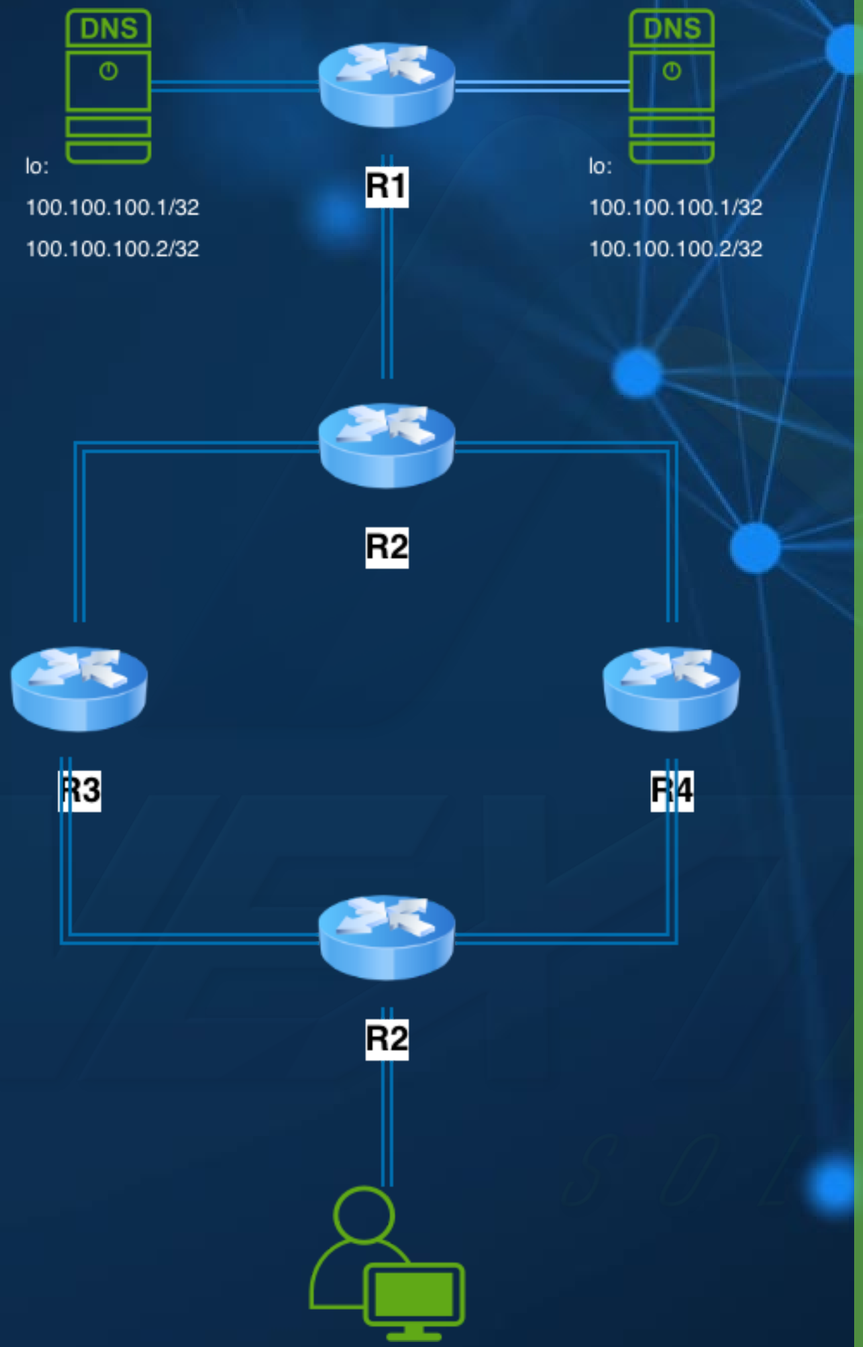
Quais sintomas você pode enfrentar?

Repare que apesar do **serviço do unbound** não estar funcionando, o FRR continuará anunciando os prefixos para a rede.

Assim, as requisições continuarão a ser encaminhadas para ele, mas ele não será capaz de atendê-las.

E, se o cenário for ECMP, isso acontecerá **apenas com PARTE das requisições**, o que pode dificultar bastante o troubleshooting.

Então além de monitorar a máquina, você DEVE MONITORAR O SERVIÇO.



GTER 51 | 2022
SÃO PAULO

Monitore

Um shell script e o crontab resolvem o problema.

E há diversas formas de realizar o monitoramento do serviço.

O que você deve saber, é que quando for detectada alguma anomalia no serviço, o seu **FRR DEVE PARAR DE ANUNCIAR OS PREFIXOS PARA A REDE**, deixando assim de receber requisições que não será capaz de atender.

Há vários tutoriais e várias formas de realizar esse processo.

O mais simples: Teste requisições localmente, em caso de falha, **PARE O SERVIÇO DO FRR**.

GTER 51 | 2022
SÃO PAULO

Monitore

Script em **/usr/bin/dns-check.sh e no crontab (crontab -e)**

```
#!/bin/bash
# Adicione ao crontab: * * * * * /usr/bin/dns-check.sh >/dev/null 2>&1


DNSUP=`/usr/bin/dig @127.0.0.1 localhost. A +short`
HOSTNAME=`hostname`
if [ "$DNSUP" != "127.0.0.1" ];
then
echo "Parando serviços de roteamento."
/etc/init.d/frr stop
/usr/bin/telegram "Node do DNS com problemas ( $HOSTNAME ). O FRR
foi finalizado. Verifique manualmente!"
fi
```

GTER 51 | 2022
SÃO PAULO

Notifique

Seja por email, telegram ou qualquer outra plataforma... notifique o seu time quando um node parar de funcionar. (Não se desespere, seu script já parou o serviço de roteamento e muito provavelmente seus clientes sequer sentirão a falha).

Se você optar por email, escolha o mutt. Ele é bem leve e simples de ser configurado.

http://www.mutt.org

Notifique

Se optar por telegram, você precisará do pacote curl, do TOKEN do seu bot e do ID do chat que você deseja enviar as notificações (pode ser grupo).

```
$ apt install curl
```

```
#!/bin/bash

#Script de Notificaçao Telegram
TOKEN="AQUI-VAI-O-TOKEN-DO-SEU-BOT"

# Configure o ID do Chat
CHAT="-1000000000"
MESSAGE=$1

curl --silent --output /dev/null
"https://api.telegram.org/bot$TOKEN/sendMessage?chat_id=$CHAT&text=$MESSAGE"

exit 0
```

E quando não estiver fazendo nada...

MONITORE!!!

```
Queries: 2804 new, 341278 total

Sources              Count      %   cum%
---------------  ---------  ------ ------
100.127.208.239      96919   28.4   28.4
                     12039    3.5   31.9
100.127.203.211       1791    0.5   32.5
100.127.227.248       1707    0.5   33.0
100.127.197.130       1697    0.5   33.4
100.127.213.76        1488    0.4   33.9
100.127.216.175       1120    0.3   34.2
100.127.211.103       1003    0.3   34.5
100.127.249.240        865    0.3   34.8
100.127.204.219        807    0.2   35.0
100.127.227.219        744    0.2   35.2
100.127.200.154        588    0.2   35.4
100.127.213.35         552    0.2   35.5
100.127.234.106        544    0.2   35.7
100.127.218.182        520    0.2   35.9
100.127.196.230        484    0.1   36.0
100.127.255.49         471    0.1   36.1
100.127.210.194        462    0.1   36.3
100.127.243.191        453    0.1   36.4
100.127.195.240        450    0.1   36.5
100.127.250.216        420    0.1   36.7
100.127.230.73         407    0.1   36.8
100.127.204.83         388    0.1   36.9
100.127.208.123        384    0.1   37.0
100.127.222.225        382    0.1   37.1
```

GTER 51 | 2022
SÃO PAULO

NEXTHOP SOLUTIONS

NETWORK EDUCATION

GTER 51 | 2022
SÃO PAULO

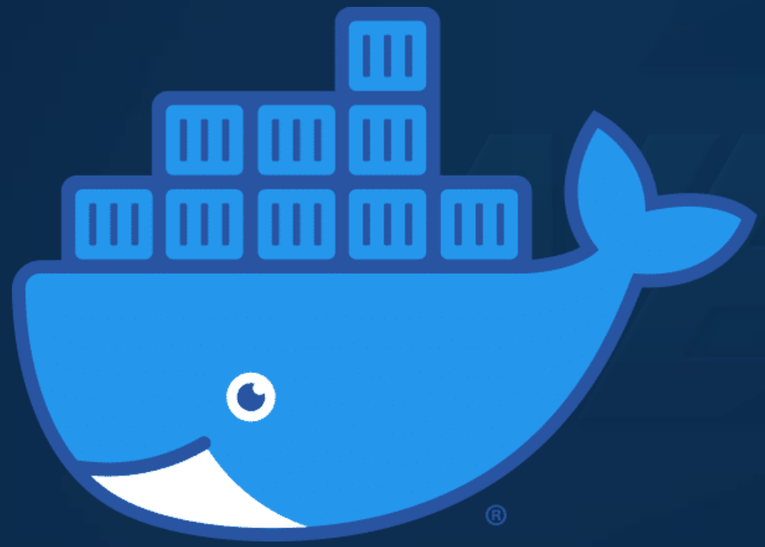
AMBIENTE DOCKER

TÉCNICAS E CUIDADOS ADICIONAIS

Docker no DNS

O processo de implementação de um DNS Recursivo Anycast é bastante trabalhoso, e por isso é muito comum que administradores optem por rodar esses cenários em containers.

E se você deseja fazer isso, deve se atentar à outros detalhes.



GTER 51 | 2022
SÃO PAULO

Docker no DNS

1 - NUNCA use a rede padrão do Docker.

A rede padrão do Docker, além de não possuir uma série de recursos disponíveis nas redes criadas pelos usuários, **FAZ NAT**.

Sim, quando você instala o Docker, a forma padrão de comunicação entre a máquina host e os containers é através de uma bridge chamada bridge0 e a comunicação externa se dá através do NAT.

iptables -L -t nat

:)

Docker no DNS

2 - Use uma rede criada por você e prefira o driver macvlan

Em uma rede criada por você é possível especificar a range, o ip fixo do container e até mesmo o prefixo IPv6.

Com o driver macvlan você será capaz de dar um bypass na gerência de rede da máquina host, entregando o endereço público diretamente para o container.

```
docker network create -d macvlan \
    --subnet=SEU-PREFIXO-PÚBLICO \
    --gateway=GATEWAY-DO-CONTAINER \
    -o parent=INTERFACE.VLANID NOME-DA-REDE-IPV4
```

O mesmo vale para rede IPv6, bastando adicionar o parâmetro --ipv6 ao comando.

GTER 51 | 2022
SÃO PAULO

Docker no DNS

3 - Crie o container adicionando-o a rede criada anteriormente. Para que seu container possa "falar ospf" você precisará do modo privilegiado durante o RUN (--privileged)

```
docker run -dit --restart unless-stopped \
    --name nome-do-node \
    --hostname hostname-do-node \
    --privileged \
    --network NOME-DA-REDE-IPV4 \
    --ip SEU-IP-DE-WAN \
     ...
```

Docker no DNS

4 - Atenção a forma como você inicializa processos.

Quem já tentou iniciar diversos processos durante a criação de um container sabe que nem sempre é uma tarefa fácil. E esse é nosso caso aqui.

Para resolver esse problema, muitos optam (inclusive eu) por utilizar o supervisor.

O supervisor é um software feito justamente para que os usuários tenham controle e possam monitorar processos em um ambiente linux.

Ele também nos permite tomar ações em caso de falha.

Site Oficial: http://supervisord.org

GTER 51 | 2022
SÃO PAULO

Docker no DNS

4 - Atenção a forma como você inicializa processos.

Acontece que, dependendo do código de saída quando o frr for parado, **o supervisor poderá tentar iniciá-lo novamente**, fazendo com que os prefixos voltem a ser anunciados pra rede.

Então, ao configurar o supervisor não esqueça de adicionar a opção autorestart=false no processo do FRR.

http://supervisord.org/configuration.html?highlight=autorestart

Docker no DNS

supervisord.conf

```
[supervisord]
nodaemon=true

[program:unbound]
command=/usr/sbin/unbound -c /etc/unbound/unbound.conf -d

[program:zabbixagent]
command=/usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf -f

[program:frr]
command=/usr/lib/frr/watchfrr zebra ospfd staticd
autorestart=false

[program:cron]
command=/usr/sbin/cron -f
```

GTER 51 | 2022
SÃO PAULO

CONSIDIDERAÇÕES FINAIS

E AGRADECIMENTOS...

Considerações Finais

- Manter um bom serviço de DNS Recursivo na sua rede é o melhor para ela, seus clientes agradecem.
- Todos os cuidados descritos nessa apresentação são cuidados que você deve tomar ALÉM dos que deveriam ser "padrão".
- Existem boas soluções comerciais no mercado, mas você pode desenvolver soluções tão eficientes quanto, invista em conhecimento.
- Não implante nada na sua rede sem dominar o assunto por completo, você pode tentar resolver um problema criando outro.
- Tenha como mantra o princípio KISS.

GTER 51 | 2022
SÃO PAULO

Agradecimentos

- Rubens Kull
- Fernando Frediani
- Toda equipe da NextHop Solutions
- Alunos e Instrutores da Network Education

GTER 51 | 2022
SÃO PAULO

nic.br | registro.br

NETWORK EDUCATION

ix.br

nic.br

SAGE NETWORKS

NEXTHOP SOLUTIONS

OBRIGADO!

ENDEREÇO PARA CORRESPONDÊNCIA

Av. Centenário, 585 - Sala 707
Unique Business Center - Torre II
Gravataí - RS - CEP: 94035-240

E-MAIL

elizandro@nexthop.solutions

TELEFONE | WHATS

(51) 99871-8111