KINDNS

DNS e KINDNS

Segurança, resiliência e qualidade.

Alguns pilares da **Internet**:

- **BGP (Border Gateway Protocol)**: protocolo que sustenta a comunicação dentro da Internet.
- **DNS (Domain Name System)**: serviço responsável pela, consulta, tradução de nome para IP e vice-versa, bem como na autenticação de segurança para emissão de certificados digitais como Let's Encrypt, **DANE** (DNS-based Authentication of Named Entities), **DNSSEC** (Domain Name System Security), **DKIM** (DomainKeys Identified Mail), **DMARC** (Domain-based Message Authentication, Reporting & Conformance), etc.

A **segurança digital** é algo que precisa de atenção e as boas práticas foram criadas para nos ajudar nesse sentido também. Algumas iniciativas globais surgiram para nos ajudar com a segurança:

- **MANRS (Mutually Agreed Norms for Routing Security)**: hoje coordenado pela **Global Cyber Alliance**, tem como objetivo aumentar a segurança do roteamento global na Internet.
- **KINDNS (Knowledge-Sharing Instantiating Norms for DNS and Naming Security)**: Assim como o MANRS, o KINDNS é uma iniciativa global criada pela **ICANN** (Internet Corporation for Assigned Names and Numbers), para trazer segurança para os operadores de DNS.

KINDNS

KINDNS

O **KINDNS** vem para ajudar na conformidade e segurança que devemos ter com nossos DNS(s), sejam eles Autoritativos ou Recursivos. As recomendações são separadas por modalidade de uso:

- **Recursivos**: **Private Resolvers**, **Shared Private Resolvers** e **Public Resolvers**.
- **Autoritativos**: **TLDs & Critical Zones** e **Other SLD Zones**.

Nesta palestra falaremos especificamente sobre **DNS(s) Recursivos na modalidade Shared Private Resolvers**, as 7 práticas recomendadas pelo **KINDNS**, alguns cases que a **ISPFocus** tem realizado e trabalhado para melhorar a Internet no Brasil.

As práticas:

- Prática 1: A **validação DNSSEC DEVE** estar habilitada para resolvedores recursivos.
- Prática 2: Declarações **ACL DEVEM** ser usadas para restringir quem pode enviar consultas recursivas para seus resolvedores/validadores DNS.
- Prática 3: (**Consideração de privacidade**): A **minimização de QNAME DEVE** estar habilitada para mitigar vazamento de nomes de domínio.
- Prática 4: Serviços DNS **autoritativo e recursivo NÃO DEVEM** coexistir no mesmo servidor DNS.
- Prática 5: Seus serviços de recursão **DEVEM ter resiliência**, usando pelo menos dois servidores distintos que considerem diversidade.
- Prática 6: O **monitoramento dos serviços, servidores e equipamentos de rede** que compõem sua infraestrutura DNS **DEVE ser implementado**.
- Prática 7: (**Consideração de privacidade**): **DoT (DNS-over-TLS) ou DoH (DNS-over-HTTPS) DEVEM** ser habilitados. Implantar qualquer um deles é a forma mais fácil de proteger contra espionagem e manipulação de consultas DNS e ataques man-in-the-middle, criptografando as consultas DNS entre stub e resolvedores recursivos, ou entre um resolvedor encaminhador e um resolvedor recursivo.

KINDNS

Neste artigo ensino como instalar um **DNS Recursivo Anycast Hyperlocal** com o **Unbound** para atender as **7 práticas** do **KINDNS**:

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

Consultas do **tipo ANY**, permitem amplificar os **ataques DDoS**. No **Unbound** é a instrução: **deny-any: yes**, faz o bloqueio dessa consulta. Como curiosidade os DNS(s) da **CloudFlare** por padrão bloqueiam esse tipo de consulta e os DNS(s) do **Google** não:

```
┌─[root@shadow]─[~]─[sex dez 19 00:51:28]
└──╼ # host -t any google.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

google.com has address 172.217.29.110
google.com has IPv6 address 2800:3f0:4001:835::200e
google.com descriptive text "apple-domain-verification=30afIBcvSuDV2PLX"
google.com descriptive text "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"
google.com name server ns4.google.com.
google.com has HTTP service bindings 1 . alpn="h2,h3"
google.com descriptive text "cisco-ci-domain-verification=47c38bc8c4b74b7233e9053220c1bbe76bcc1cd33c7acf7acd36cd6a5332004b"
google.com descriptive text "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com descriptive text "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com name server ns2.google.com.
google.com descriptive text "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com descriptive text "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com mail is handled by 10 smtp.google.com.
google.com name server ns3.google.com.
google.com descriptive text "v=spf1 include:_spf.google.com ~all"
google.com name server ns1.google.com.
google.com has CAA record 0 issue "pki.goog"
google.com descriptive text "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com descriptive text "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com has SOA record ns1.google.com. dns-admin.google.com. 846175965 900 900 1800 60
google.com descriptive text "onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"
google.com descriptive text "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
┌─[root@shadow]─[~]─[sex dez 19 00:51:31]
└──╼ #
```

Fazendo a mesma consulta pelo 1.1.1.1:

```
┌─[root@shadow]─[~]─[sex dez 19 00:56:38]
└──╼ # host -t any google.com 1.1.1.1
Using domain server:
Name: 1.1.1.1
Address: 1.1.1.1#53
Aliases:

Host google.com not found: 4(NOTIMP)
┌─[root@shadow]─[~]─[sex dez 19 00:56:53]
└──╼ #
```

KINDNS

Prática 6 - **Monitoramento**

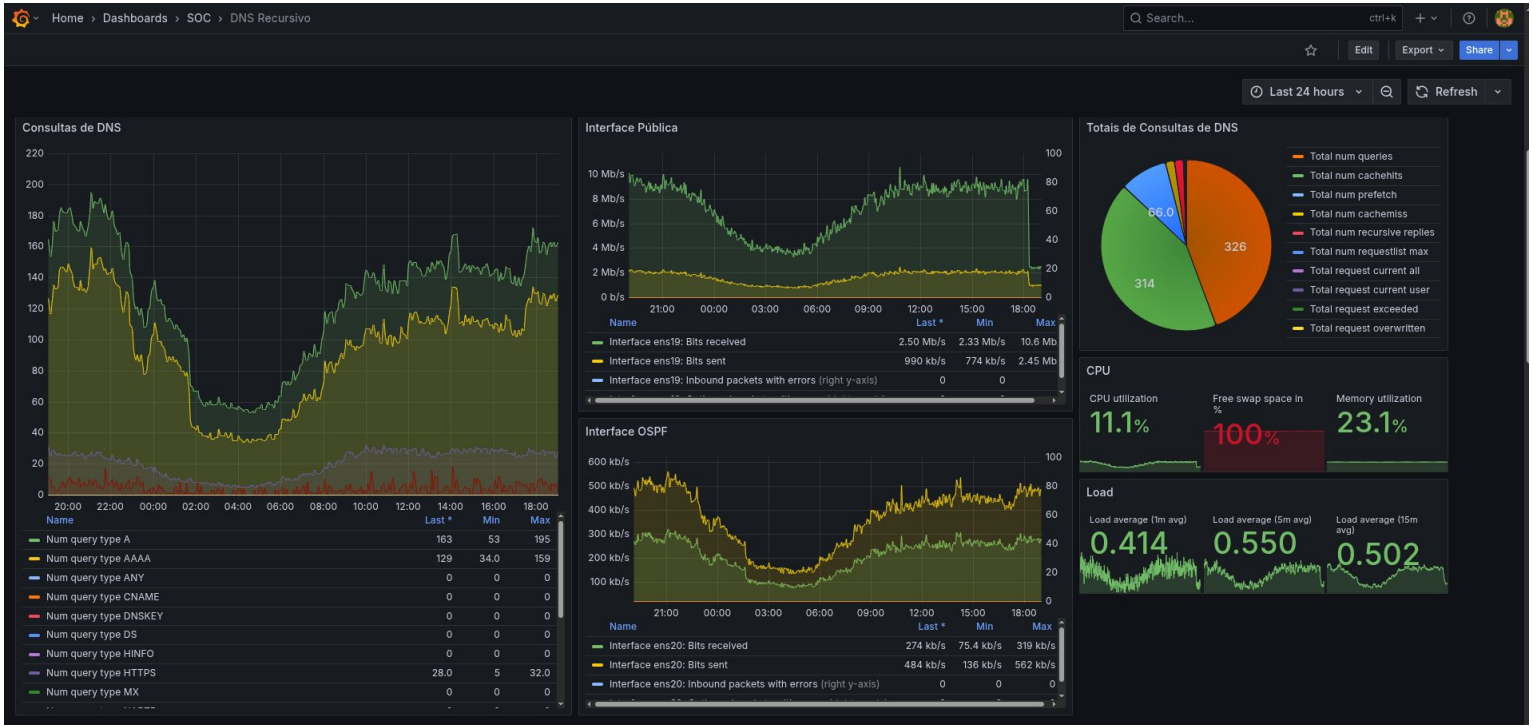
O monitoramento do seu serviço DNS é fundamental para garantir que ele esteja disponível para usuários e clientes. Isso pode ser feito por meio de monitoramento local (hospedado internamente) ou a partir de um local remoto, e pode ser gerenciado por você mesmo ou por um terceiro (terceirizado/ baseado em nuvem).

O que podemos e devemos monitorar?

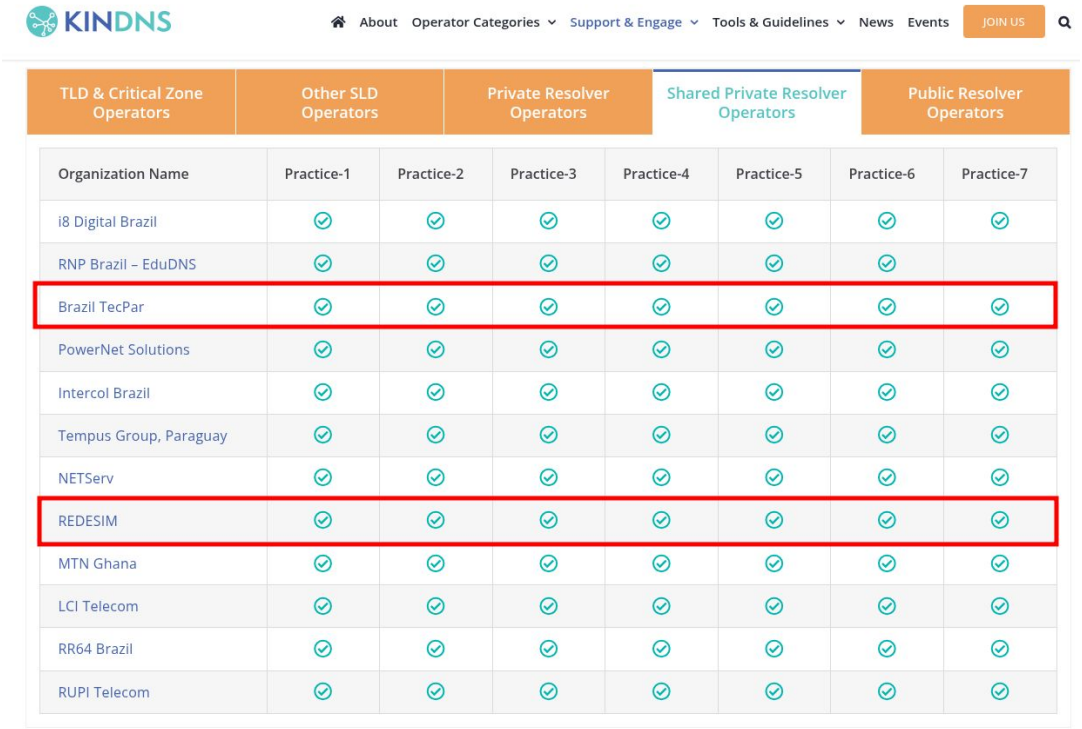
- Queries por tipos de registradores de DNS.
- Se o serviço DNS parou.
- Se o serviço de Roteamento parou: o FRRouting, BIRD, etc. Necessário para o anycast.
- Perda de pacotes.
- Latência.
- Consumo de CPU/Load/Memory/Swap/Disk.
- Recursividade IPv4 e IPv6.
- Anycast (monitorar o IGP Interior Gateway Protocol): OSPF, IS-IS, etc

KINDNS

Exemplo de monitoramento:

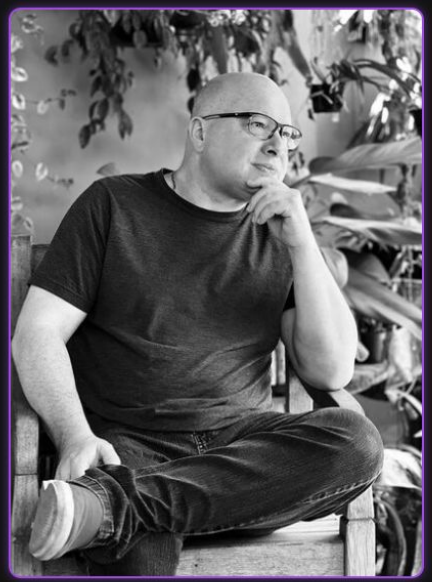


- Cases de sucesso envolvendo **DNS(s) Recursivos Anycast Hyperlocal** atendendo as 7 práticas do **KINDNS**:



Organization Name	Practice-1	Practice-2	Practice-3	Practice-4	Practice-5	Practice-6	Practice-7
i8 Digital Brazil	✓	✓	✓	✓	✓	✓	✓
RNP Brazil – EduDNS	✓	✓	✓	✓	✓	✓	
Brazil TecPar	✓	✓	✓	✓	✓	✓	✓
PowerNet Solutions	✓	✓	✓	✓	✓	✓	✓
Intercol Brazil	✓	✓	✓	✓	✓	✓	✓
Tempus Group, Paraguay	✓	✓	✓	✓	✓	✓	✓
NETServ	✓	✓	✓	✓	✓	✓	✓
REDESIM	✓	✓	✓	✓	✓	✓	✓
MTN Ghana	✓	✓	✓	✓	✓	✓	✓
LCI Telecom	✓	✓	✓	✓	✓	✓	✓
RR64 Brazil	✓	✓	✓	✓	✓	✓	✓
RUPI Telecom	✓	✓	✓	✓	✓	✓	✓

Sobre mim e meus contatos



Marcelo Gondim da Cunha

Especialista em redes e segurança, com experiência desde os anos 1990. Atuou como desenvolvedor, consultor de sistemas GNU/Linux e foi CTO da Nettel Telecom, onde implantou IPv6 em 2013. Contribui com o projeto MANRS. Também liderou o SOC da Brasil TecPar entre 2022 e 2025, focando em defesas contra DDoS, boas práticas e onde desenvolveu uma rede de DNS(s) Recursivos Anycast certificada pelo KINDNS.

- Administração de Sistemas Unix-Like desde 1996.
- Consultor na Conectiva S/A - Unidade Rio em 2000.
- Direção do AS53135 - Nettel Telecomunicações entre 2003 e 2021 atingindo a marca de 41.000 assinantes.
- Diversas palestras em eventos da área de Redes e Serviços e artigos técnicos publicados.

KINDNS

Apresentação em memória de:

Rubens Kühl

Danton Nunes

Liane Tarouco