DNS e algumas extensões KINDNS

Daniel Fink
daniel.fink@icann.org

IX Fórum
26 de outubro de 2022

Por que?

KINDNS

Desde a RFC882 (1983) o protocolo DNS mudou bastante.

- De acordo com “DNS Camel Viewer” (PowerDNS):
  - 297 RFCs relevantes ao DNS
  - 2.082 páginas de texto

- Mudanças incluem:
  - Adições majoritárias (DNSSEC)
  - Novos RR’s
  - Mecanismos de privacidade (QTYPE minimization)
  - …muito mais

Desafios para operadores

KINDNS

- DNS ficou complexo, muitas escolhas e implementações.
- Provedores necessitam um serviço de DNS seguro e rápido.
  - Mas apenas especialistas conseguem conhecer o protocol em profundidade.

Desafios para operadores

KINDNS

- Como um pequeno provedor pode acompanhar novidades como DoH, DoT, DoQ, DoHoT e seus impactos?
- Como manter-se atualizado sobre as últimas recomendações de segurança?
- Como saber se devo implementar validação DNSSEC e escolher as chaves criptográficas?
- Como um gerente pode especificar os requisitos mínimos para terceirizar serviços ?

O que é?

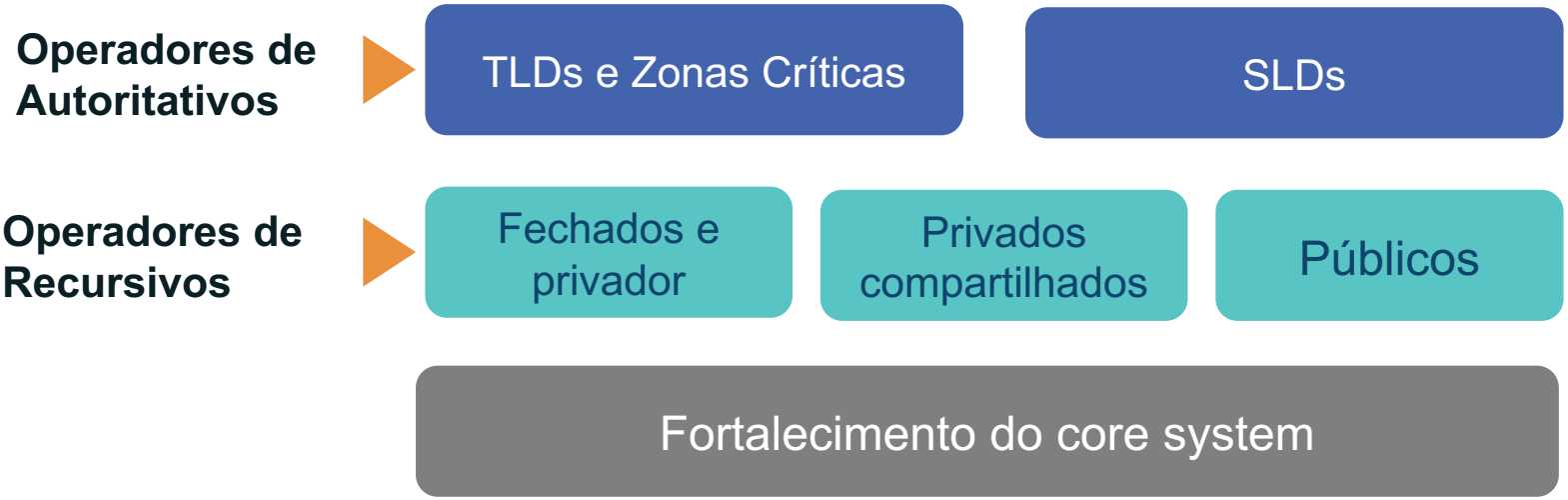
As Normas de Compartilhamento de Conhecimento e Instanciamento para DNS e Segurança de Nomes de Domínio (KINDNS) é uma iniciativa da ICANN para compartilhar de uma forma simples e clara as melhores práticas operacionais para operadores de DNS.

KINDNS

Knowledge-sharing and
Instantiating
Norms for
DNS (Domain Name System) and
Naming
Security

Normas de Compartilhamento de Conhecimento e Instanciamento para DNS e Segurança de Nomes de Domínio

Para quem?



Ao aderir à iniciativa KINDNS, os operadores de DNS comprometem-se voluntariamente a aderir às práticas identificadas e a agir como “embaixadores da boa vontade” dentro da comunidade.

Operadores de Autoritativos para SLDs

KINDNS

SLDs

1. **DEVE** ser assinada pelo DNSSEC e seguir as práticas recomendadas de gerenciamento de chaves.
2. A transferência de zonas entre servidores autoritativos **DEVE** ser limitada.
3. A integridade do arquivo de zona **DEVE** ser controlada.
4. Servidores de nomes autoritativos e recursivos **DEVEM** ser executados em infraestruturas separadas.
5. Um mínimo de dois servidores de nomes distintos DEVE ser usado para qualquer zona.
6. Servidores autoritativos para uma determinada zona DEVEM ser executados a partir de infraestrutura diversificada
7. A infraestrutura **DEVE** ser monitorada

Operadores de Recursivos Privados e Compartilhados

KINDNS

Os operadores de recursivos privados compartilhados geralmente são provedores de serviços de Internet (ISPs).

Recursivos Privados Compartilhados

1. A validação DNSSEC **DEVE** estar ativada
2. As instruções ACL **DEVEM** ser usadas para restringir quem pode enviar consultas recursivas
3. A minimização de QNAME **DEVE** estar ativada
4. Servidores de nomes autoritativos e recursivos **DEVEM** ser executados em infraestrutura separada.
5. Pelo menos dois servidores distintos **DEVEM** ser usados para fornecer serviços de recursão
6. A infraestrutura **DEVE** ser monitorada
7. Para consideração de privacidade: Criptografia (DOH ou DoT) **DEVE** ser ativada
8. Operadores de resolvedores privados **DEVEM** ter diversidade de software

Authoritative DNS Operators of Critical Zones

KINDNS

TLDs & Critical Zones

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive name servers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Closed and Private Resolver Operators

Private resolvers are not publicly accessible and cannot be reached over the open Internet. They are typically found in corporate networks or other restricted-access networks

Closed and Private resolvers

1. DNSSEC validation **MUST** be enabled
2. Access control list (ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive name servers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Public Resolver Operators

KINDNS

This category includes both open and closed public resolvers. Closed public resolvers are typically commercial DNS filtering/scrubbing services, such as DNSFilter and OpenDNS.

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. QNAME minimization **MUST** be enabled
3. **For** privacy considerations: Encryption (DOH or DoT) **SHOULD** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. Data collected through the passive logging of DNS queries **MUST** be limited
6. At least two distinct servers **MUST** be used for providing recursion services
7. Public resolver operators **MUST** ensure operational diversity in their infrastructure.
8. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Hardening the Core

KINDNS

Além das boas práticas para segurança do DNS, fortaleça também as plataformas dos seus sistemas.

Core Hardening

1. ACLs **DEVEM** ser implementadas para controlar tráfego de rede para os servidores de DNS
2. BCP38/MANRS egress filtering **DEVEM** ser implementadas
3. A configuração do servidor de DNS **DEVE** ser dedicada
4. Permissões de usuários e acesso de aplicações aos recursos do sistema **DEVEM** ser limitadas
5. Arquivos de configuração de sistemas e serviços **DEVEM** ser versionados.
6. Acesso ao gerenciamento de serviços **DEVE** ser restrito.
7. Acesso ao console do sistema DEVE ser protegido através de chaves criptográficas e/ou autenticação de dois fatores
8. Gerenciamento de credenciais para acesso de clientes DEVE aderir às melhores práticas.

Autoavaliação e Inscrição

1. Os operadores de cada categoria podem realizar uma autoavaliação de suas práticas operacionais em relação ao KINDNS e usar o relatório para corrigir/ajustar suas práticas.

    - As autoavaliações serão anônimas e os relatórios serão baixados diretamente do site.

2. Os operadores podem se inscrever para participar de uma ou várias categorias cobertas pelo KINDNS.

    - A participação na iniciativa KINDNS significa comprometer-se voluntariamente a implementar/aderir às práticas acordadas.
    - Os participantes tornam-se embaixadores da boa vontade e promovem as melhores práticas.

Qual é o site?

KINDNS

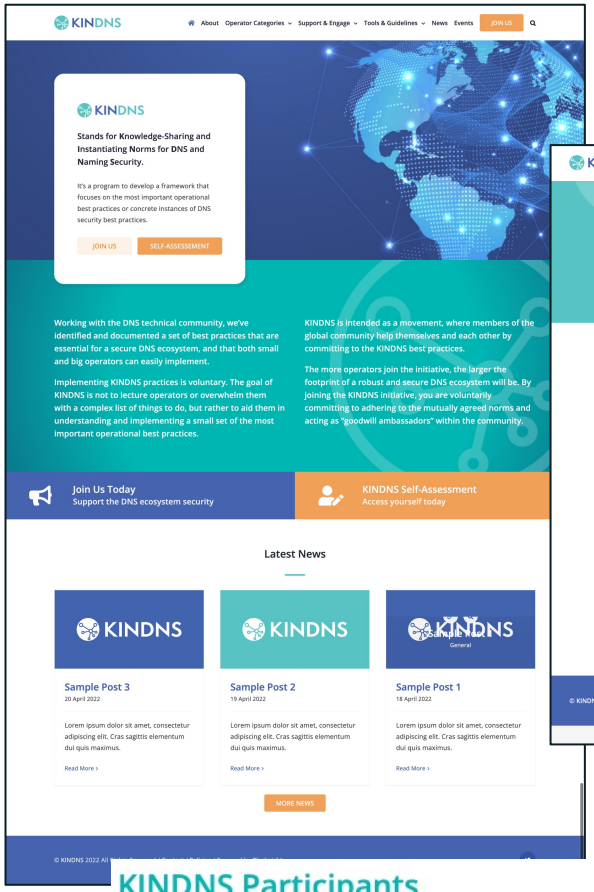
An ICANN Initiative

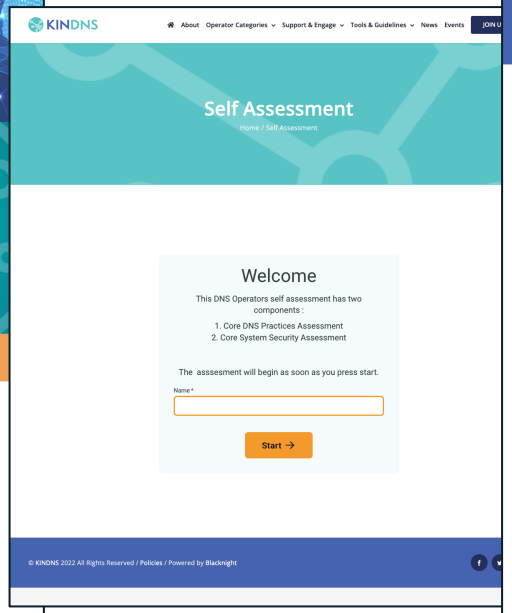
ICANN

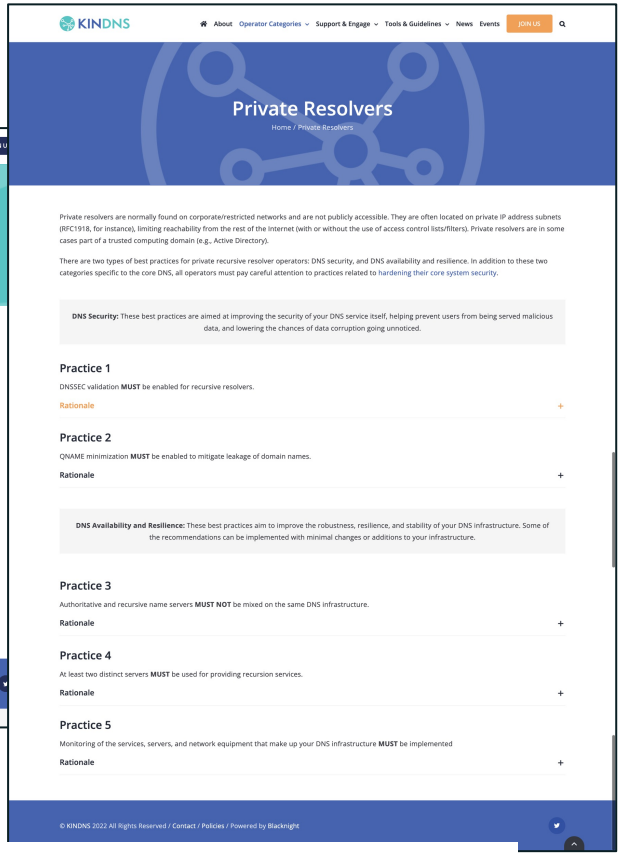
https://kindns.org

Website – kindns.org

KINDNS







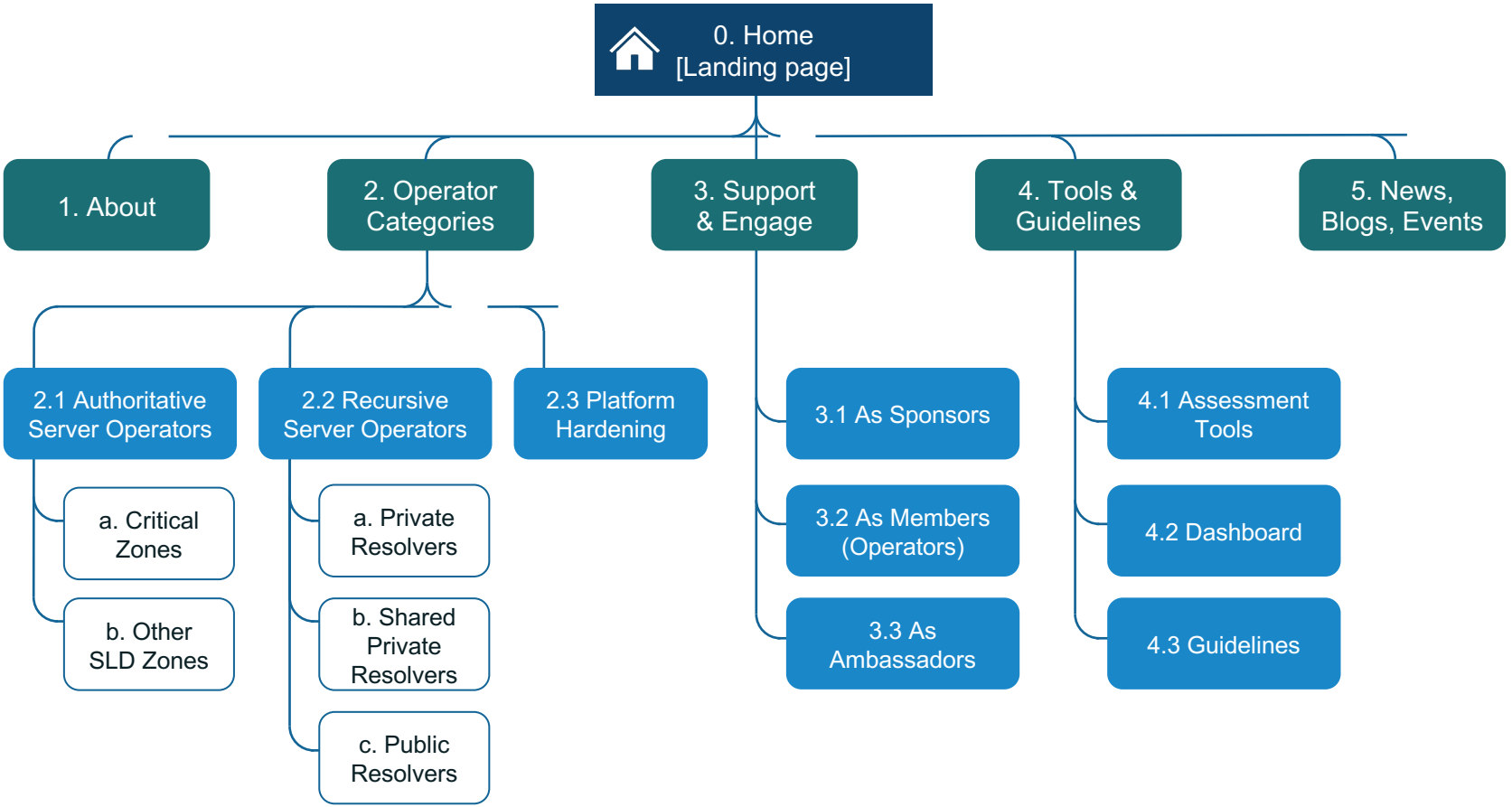
KINDNS Participants

TLD & Critical Zone Operators	Other SLD Operators	Private Resolver Operators	Private Shared Resolver Operators	Public Resolver Operators

Organization Name	Date Joined	Practice-1	Practice-2	Practice-3	Practice-4	Practice-5	Practice-6
Posix (for posix.co.za)	06 Oct 2022	✓	✓	✓	✓	✓	✓
ICANN (for icann.org)	07 Oct 2022	✓	✓	✓	✓	✓	✓

Website Map

kindns.org Site Map



Relatórios de Autoavaliação

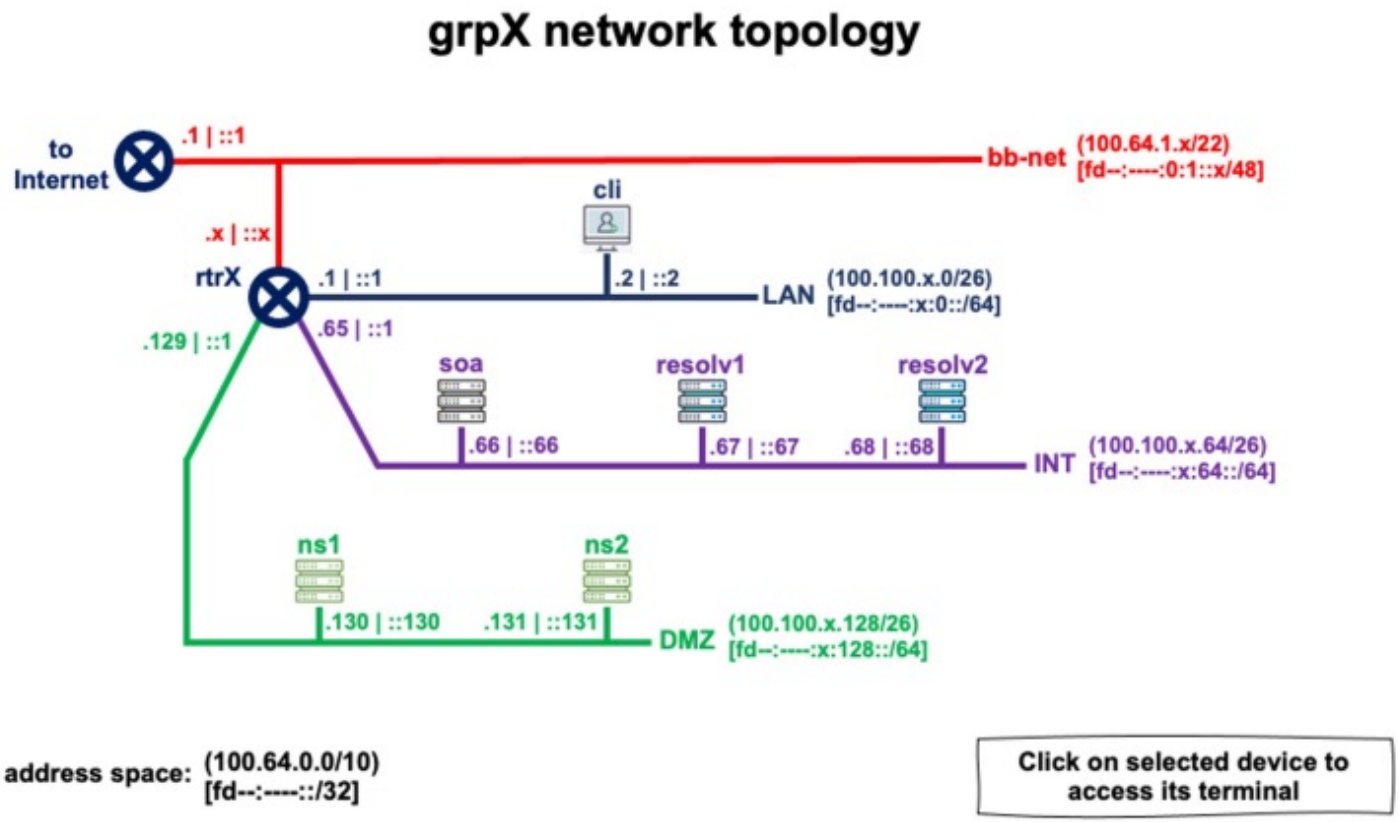
Como podemos ajudar?

Nicolás Antoniello nicolas.antoniello@icann.org

Gerente de Relacionamento Técnico

ICANN, Montevideo

Laboratório no navegador



Como se manter informado e contribuir

- https://kindns.org
- **Lista de discussão do KINDNS:**

  kindns-discuss@icann.org
- **Twitter**

  https://twitter.com/4kindns

Muito obrigado – daniel.fink@icann.org

One World, One Internet

Visit us at **icann.org**

e_Mail: kindns-info@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg