KINDNS

KINDNS

A Framework to Improve Secured DNS Operations

Aug. 2023

Yazid AKANHO
ICANN's Office of the CTO
Yazid.Akanho@icann.org

Agenda

1. KINDNS presentation
2. Demo
3. Q/R session

KINDNS

What Is It?

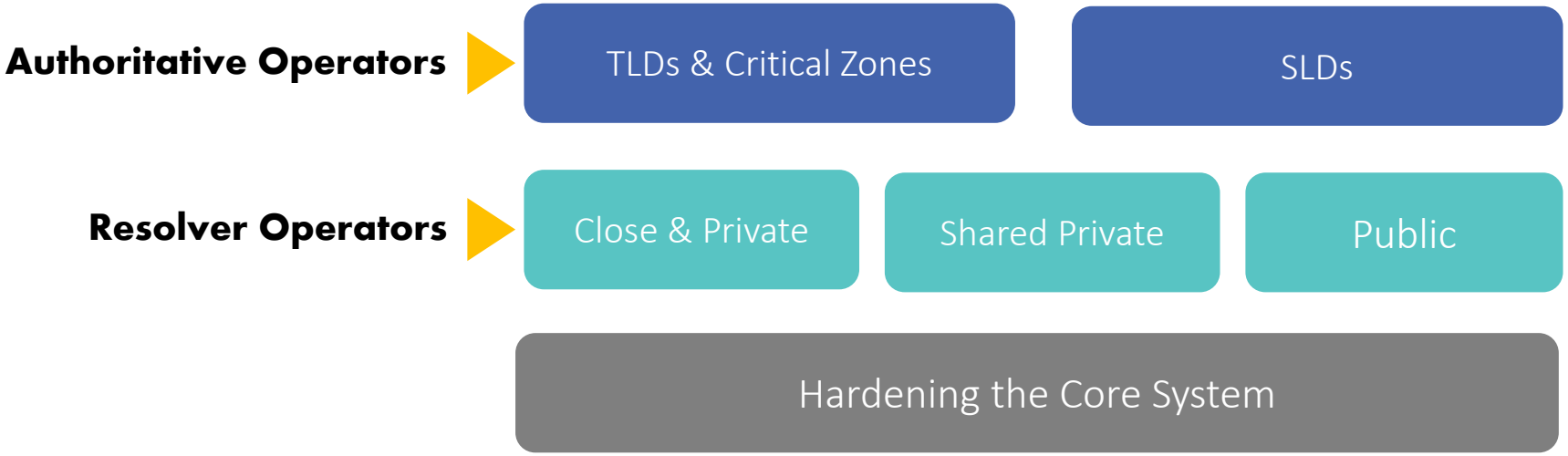
Knowledge-sharing and **I**nstantiating **N**orms for **D**NS
(Domain Name System) and **N**aming **S**ecurity

*A simple framework that can **help a wide variety of DNS operators**, from small to large, to follow both the **evolution of the DNS** protocol and the best practices that the industry identifies for better security and more effective DNS operations.*

***.....** is pronounced "**kindness**"*

KINDNS

Targeted Operators



Each category has 6-8 practices that we encourage operators to implement.
See www.kindns.org, for more details.

KINDNS

Authoritative DNS Operators of Critical Zones

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 nameservers **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

KINDNS

Authoritative DNS Operators of SLDs

SLDs

1. **MUST** be 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 nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

KINDNS

Closed & Private Resolver Operators

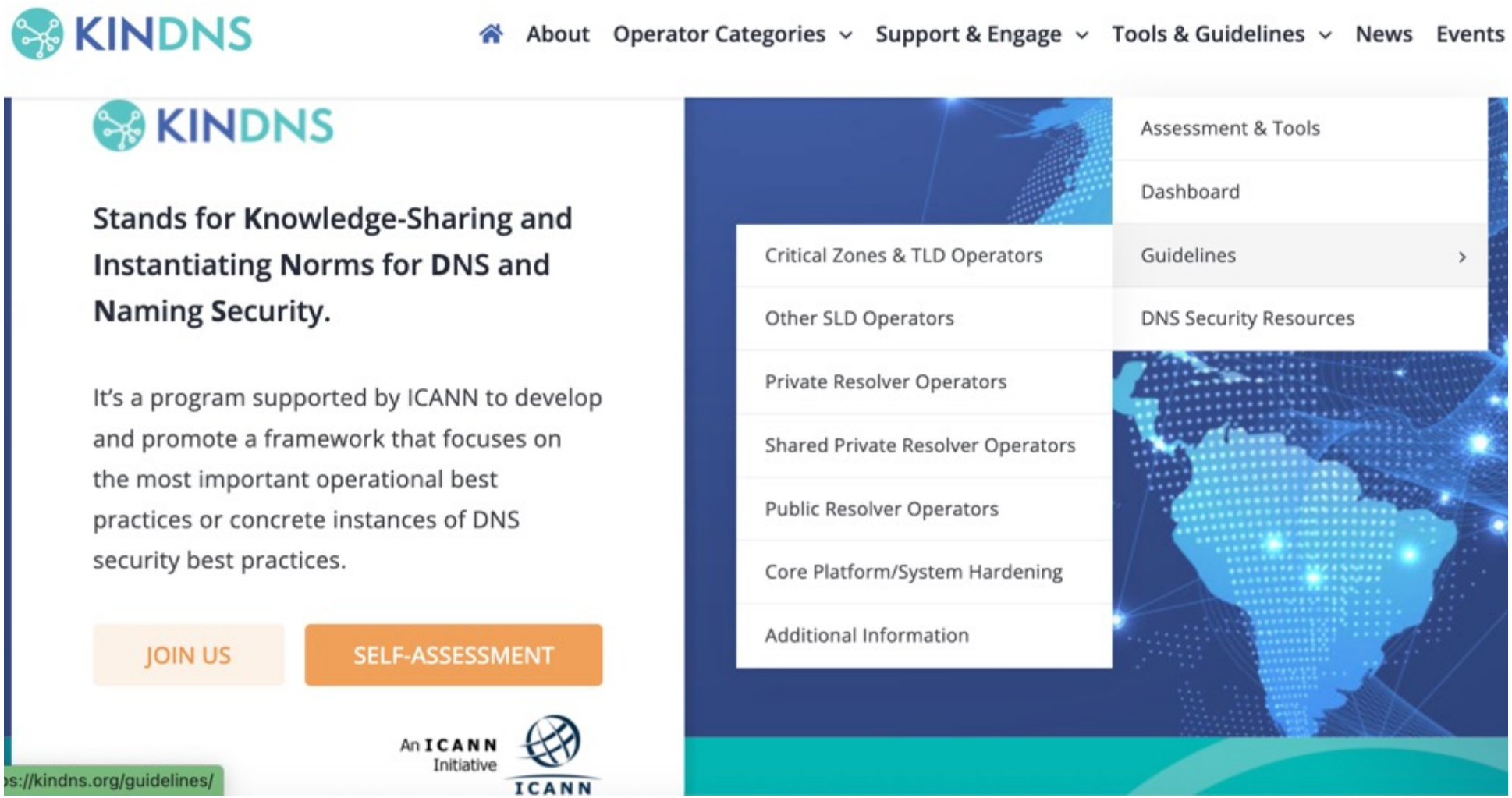
Private resolvers are not publicly accessible and cannot be reached over the open internet. They are typically found in corporate networks or other restricted-access networks

Closed & 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 nameservers **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 a diversified Infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

KINDNS

All practices are well documented there!



KINDNS

Self-assessment & Enrollment

Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices.

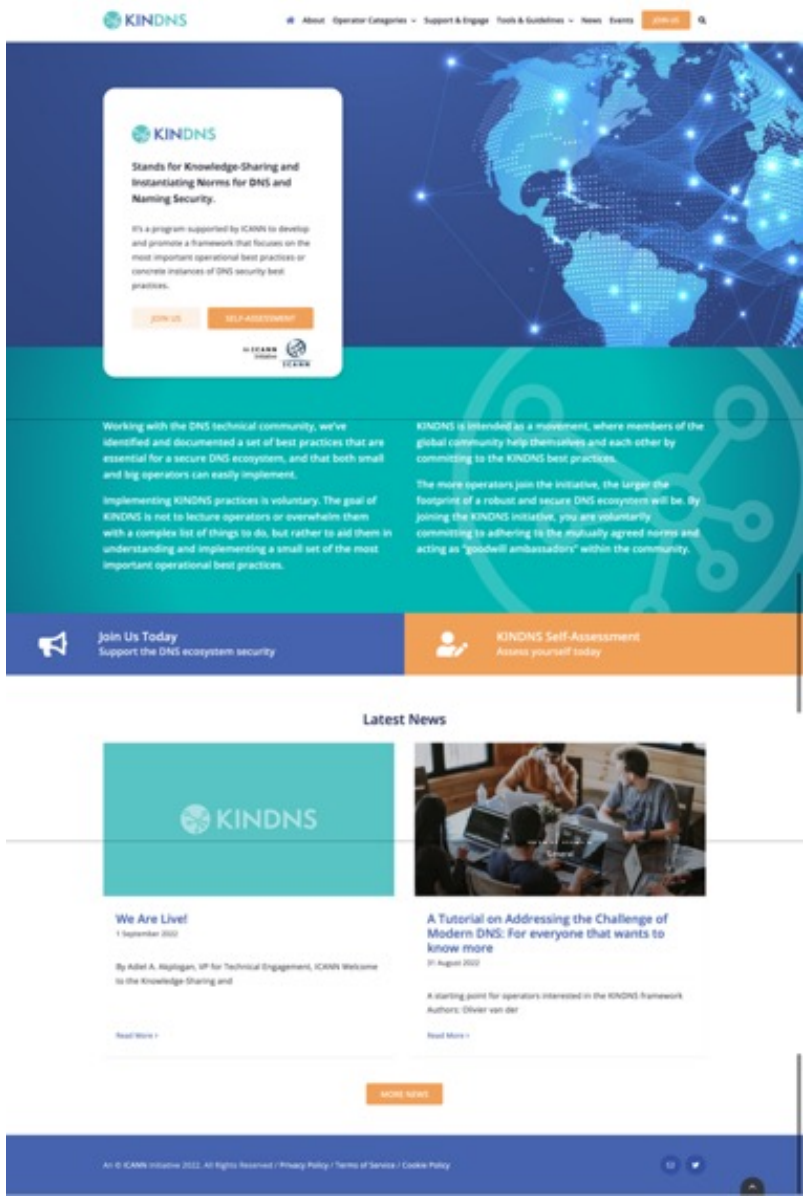
- self-assessment is anonymous
- reports can be downloaded directly from the web site.

Operators can enroll as participant to one or many categories covered by KINDNS.

- Participation in the KINDNS initiative means voluntarily committing to implement/adhere to agreed practices.
- Participants become goodwill ambassadors and promote best practices.

KINDNS

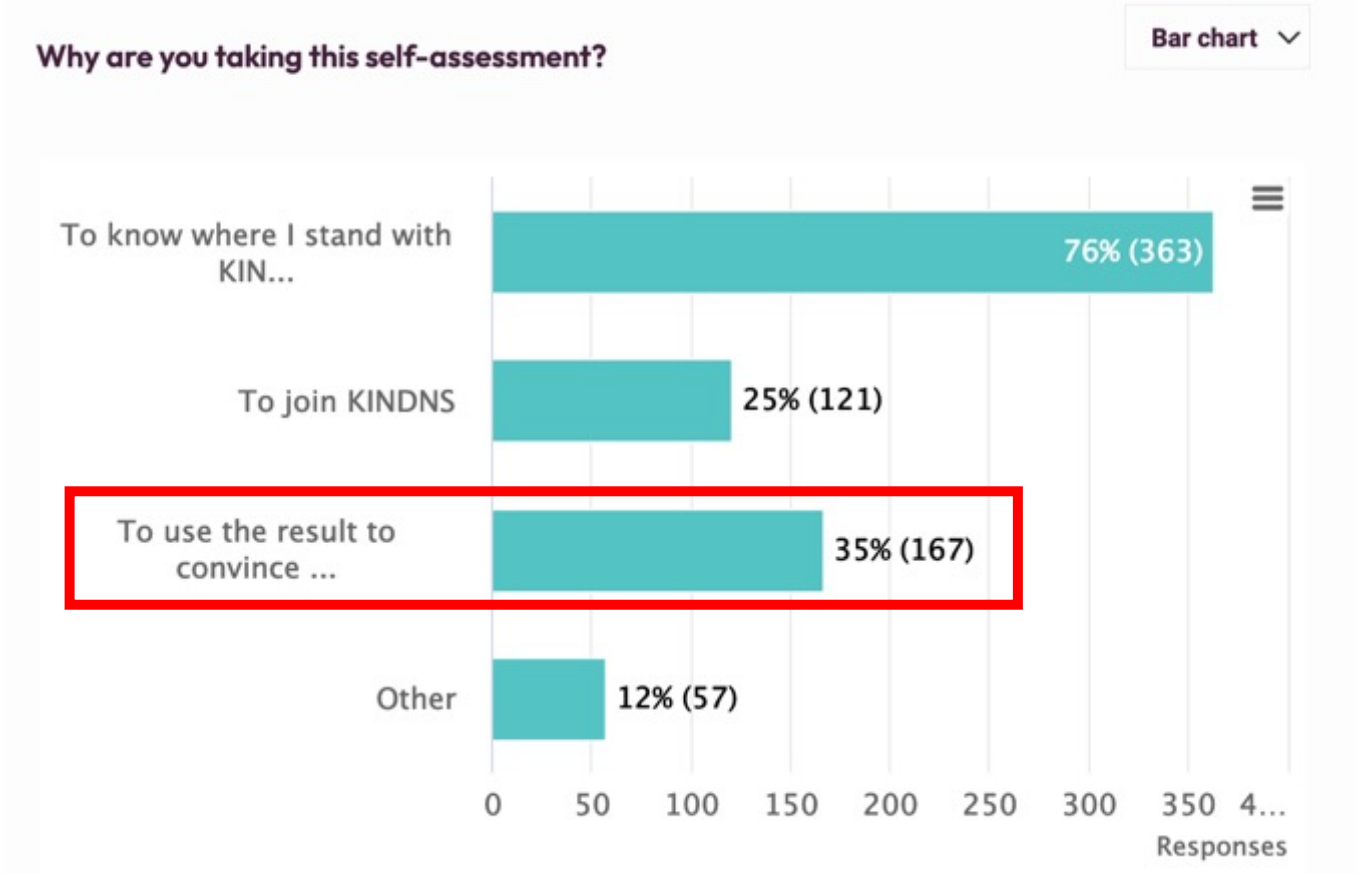
Website – https://kindns.org/

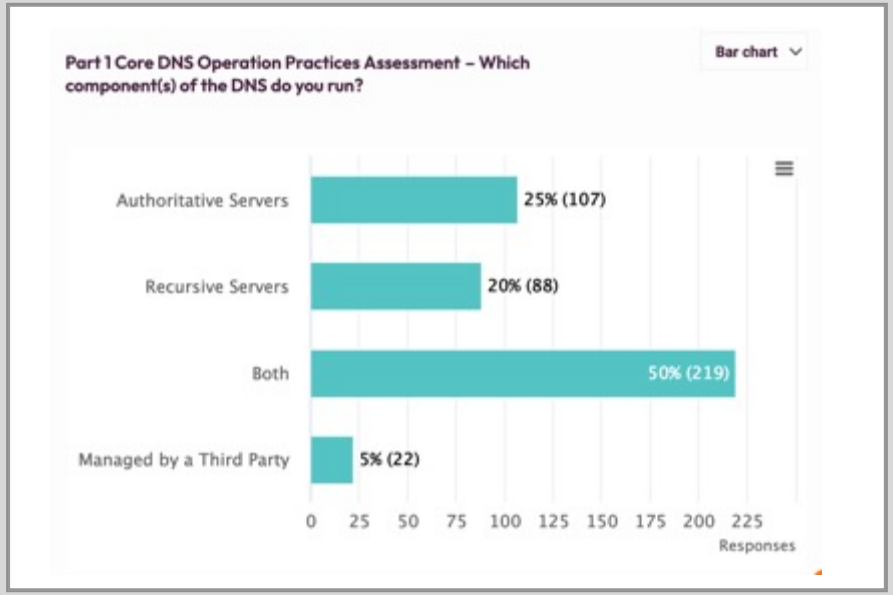


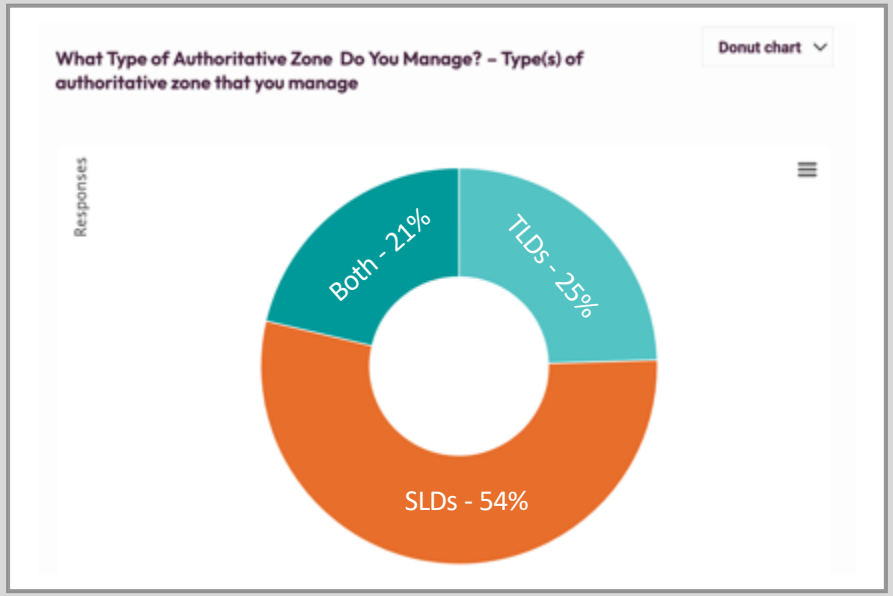
Self-Assessment Report

KINDNS

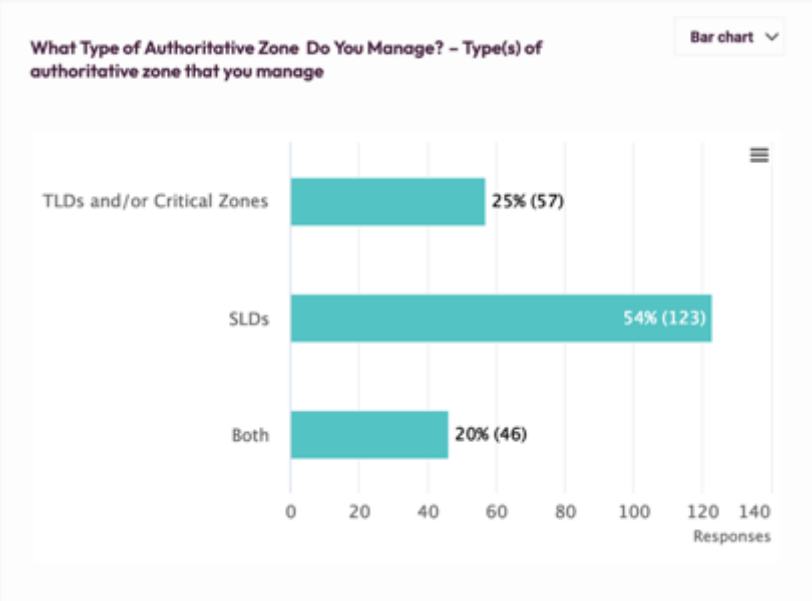
Early Observations

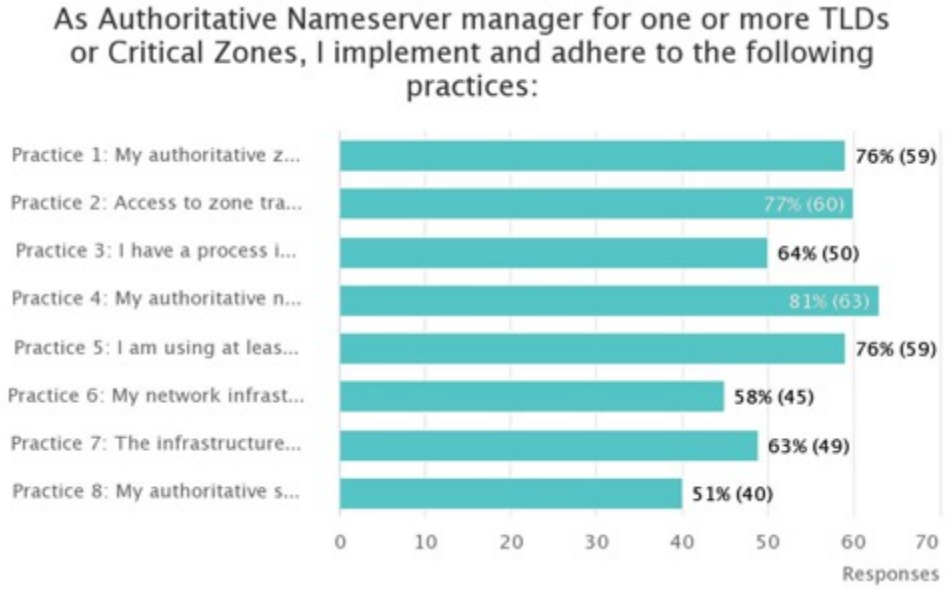


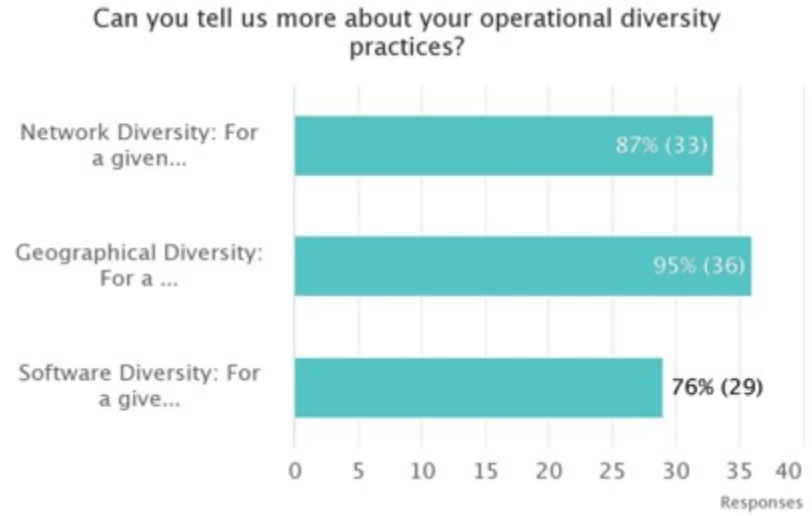


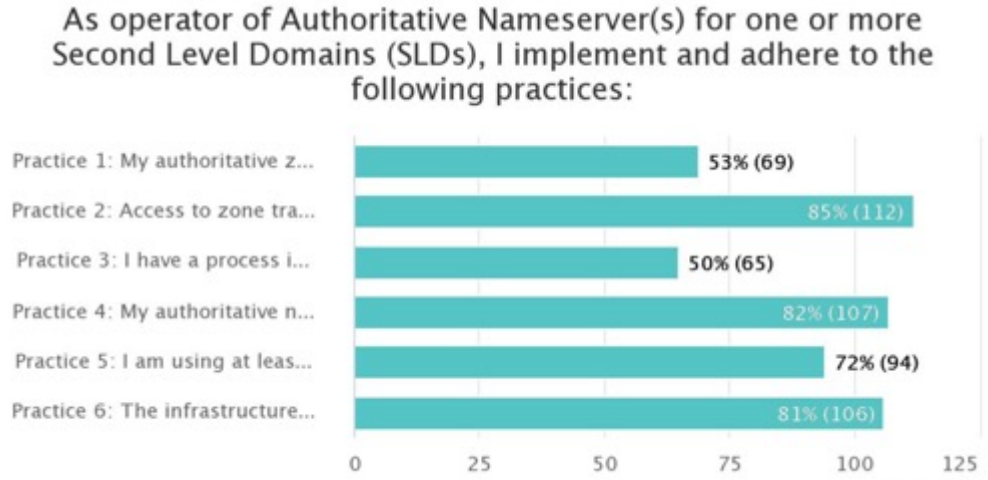


Early Observations (con't)









KINDNS

Selecting BCPs

How do we identify them ?

- Draw from own operational experience
- Ask operators (NOG lists, communities)
- Review RFCs and other standards
  https://powerdns.org/dns-camel/
- Shortlist based on relevance, ease of implementation, and how widespread the adoption is

Ask operators to review the selection (kindns-discuss)

Debate and justify choices

KINDNS

Engaging the community

Operators must agree on the selected BCPs

kindns-discuss list launched in 2021

- Encouraged operators from all backgrounds to join
- When in doubt, we asked community for advice on what they consider to be a BCP or not
- Some things were debated – is DNSSEC validation a **MUST** nowadays ? (We think so ☺)
- Some practices weren't implemented widely enough, or too complicated (not low hanging fruit) for small operators
  - e.g. Anycast

KINDNS

Current Focus: Phase 2

Service Platform Hardening

- **Front-end**
  - Re-Activate the full **enrollment form**
  - **Translate** the website and the tools into other languages
  - **Evolve the Self-assessment** tool to technically measure/assess how operators implement the practices.
    - Two views: Internal & External
    - Ability to measure implementation by collecting anonymized data from the self-assessment tool.
    - Integrate a Zonemaster version for Authoritative servers

- ***Back-end***
  - *Integrate the KINDNS server to ICANN E&I monitoring service*
  - *Implement a ticketing system to better track interactions with the public.*
  - *Improve the security fence around WordPress*
  - *Deploy an integrated enrollment management tool (a WP plugin)*
  - *Renew ICANN infosec assessment.*
  - *Directly link self-assessment to enrollment*
  - *Develop an integrated tool to simplify/automate Operator compliance assessment*

KINDNS

Current Focus: Phase 2 (con't)

Community Engagement

- **Community engagement**: continue to encourage operators to get onboard to **contribute and support** the framework:
  - *Direct 1:1 Engagements*
  - *Convince/Encourage more DNS operators to join*
  - *Workshops & webinars to raise awareness on KINDNS practices as part of our overall DNS ecosystem security awareness program*.
  - DNSAthons around secure DNS operations
  - Develop partnerships with programs such as MANRS and Pulse, internet.nl, etc.
- **Communication**: a more active communication plan to further promote KINDNS
  - Publish a series of DNS best practices dedicated blogs
  - Develop toolkits to help operators engage with internal decision-makers.

KINDNS

KINDNS v.2 - Discussion Points

1. **Adding Response Rate Limiting (RRL)** to Authoritative Servers' practice
   - ccTLD and critical Zone Operators
   - Other SLDs too?

2. **Addressing 'Split' responsibilities** for Authoritative servers' operation:
   - Zone file content is controlled by a third party. i.e root server operators and the root zone itself.

3. **Access reliability:** Reachability over IPv6, RPKI for the prefix used for the DNS servers.

4. **Community review team**: volunteers from the community to work with staff to help with assessing participating candidates or other aspect of KINDNS practice evolution.

5. **Metrics**: help measure the impact of KINDNS adoption on global DNS operations

KINDNS

Some external additional tools

1. **Zonemaster**: https://zonemaster.net/

   A program that tests a DNS zone configuration with different sanity checks configured in an engine and provides a zone health report.

2. **DNSviz**: https://dnsviz.net/

   Provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and lists configuration errors detected by the tool.

3. **SuperTool**: https://mxtoolbox.com/SuperTool.aspx

   An integrated tool that can perform several kind of diagnostics on a domain name, IP address or host name. Documentation available at https://mxtoolbox.com/restapi.aspx

4. **Intodns**: https://intodns.com/

   Checks the health and configuration and provides DNS report and mail servers report.

KINDNS

Stay Informed and Contribute

Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Mailing list	kindns-discuss@icann.org https://mm.icann.org/mailman/listinfo/kindns-discuss

KINDNS

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: kindns-info@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg