
KINDNS
KINDNS
KINDNS
pronounced kindness
ICANN
ICANN
ICANN
ICANN

KINDNS

KINDNS

An Initiative to Promote DNS Operational Best Practices

October 10th 2024

Ulrich Wisser
Regional Technical Engagement Manager, Europe
ICANN

What Is It?

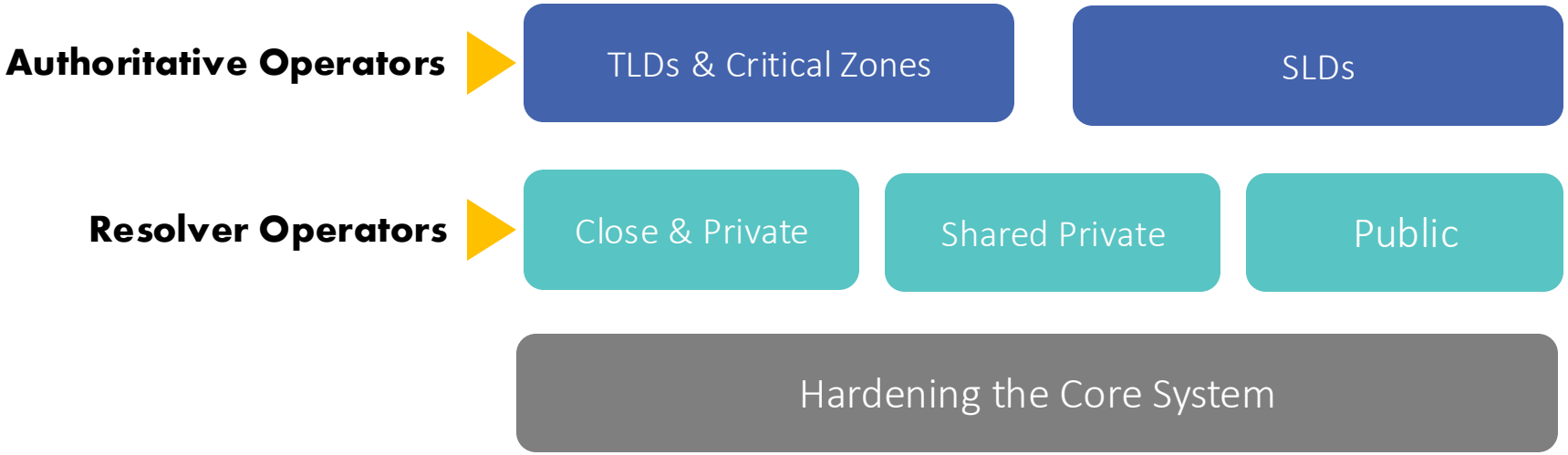
Knowledge-sharing and **I**nstantiating **N**orms for **D**NS
(Domain Name System) and **N**aming **S**ecurity

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 will encourage operators to implement. See www.kindns.org, for more details
- By joining KINDNS, DNS operators are voluntarily committing to adhere to these identified practices and act as "goodwill ambassadors" within the community.

KINDNS

Authoritative DNS Operators of Critical Zones

TLDs & Critical Zones

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. 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. The infrastructure that makes up your DNS infrastructure **MUST** be monitored
7. DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **SHOULD** be enabled

KINDNS

Public Resolver Operators

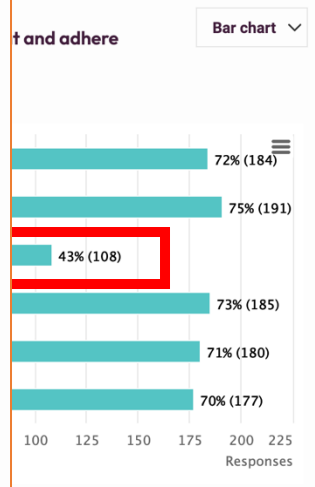
"Fully open" public DNS resolvers are available to any users on the Internet freely to use, whether they are stub resolvers (clients) or recursive servers using the open resolver as a forwarding service.

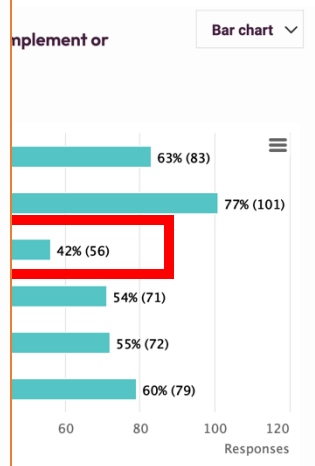
Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled
2. DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **MUST** be enabled
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. The infrastructure that makes up your DNS infrastructure **MUST** be monitored
7. DNS Query data **MUST** only be retained for as long as is necessary for the sound operation of the service offered

KINDNS

As operator of a Public Recursive Resolver, I implement or adhere to the following practices :

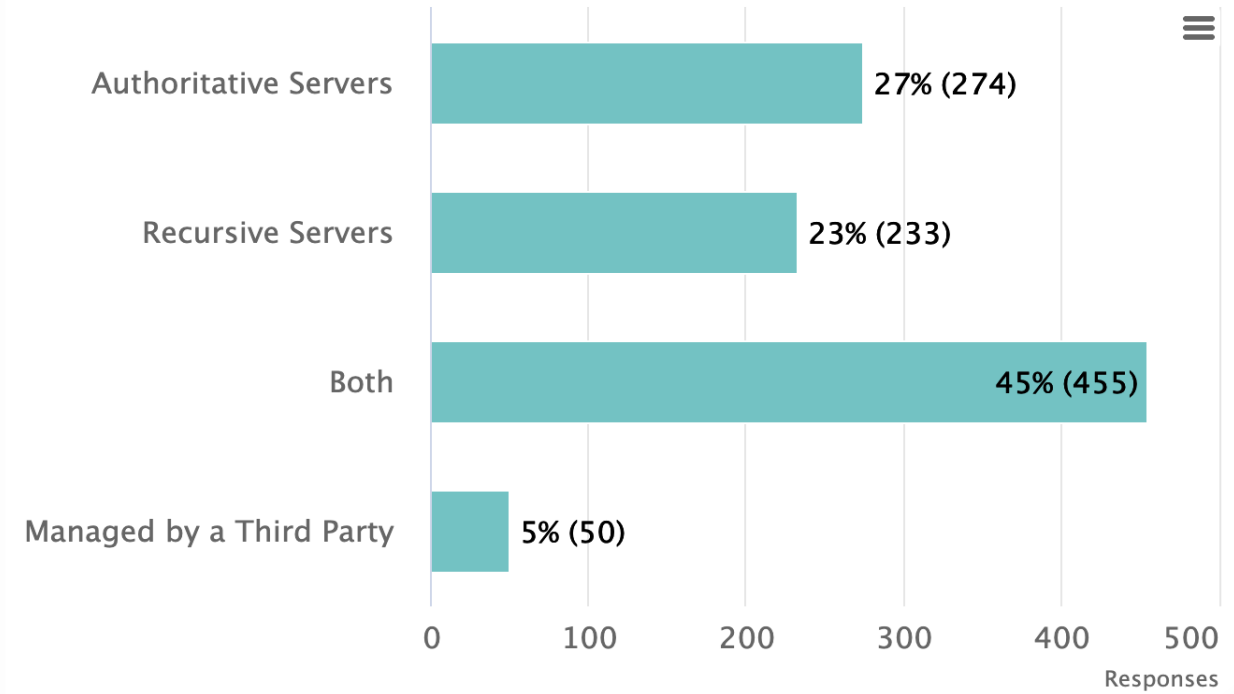




KINDNS

Part 1 Core DNS Operation Practices Assessment – Which component(s) of the DNS do you run?

Bar chart



KINDNS


Why are you taking this self-assessment?
Bar chart
To know where I stand with KIN...
74% (816)
To join KINDNS
32% (349)
To use the result to convince ...
40% (444)
Other
10% (114)
0
100
200
300
400
500
600
700
800
Responses

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, or registrars hosting DNS for registrants

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

4. **Steering Committee and Community review team**:
   - Volunteers to help steer the evolution KINDNS as framework and coordinate the initiative.

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

KINDNS