



KINDNS

An ICANN Initiative to Promote DNS Operational Best Practices

Adiel A. Akplogan

VP, Technical Engagement ICANN

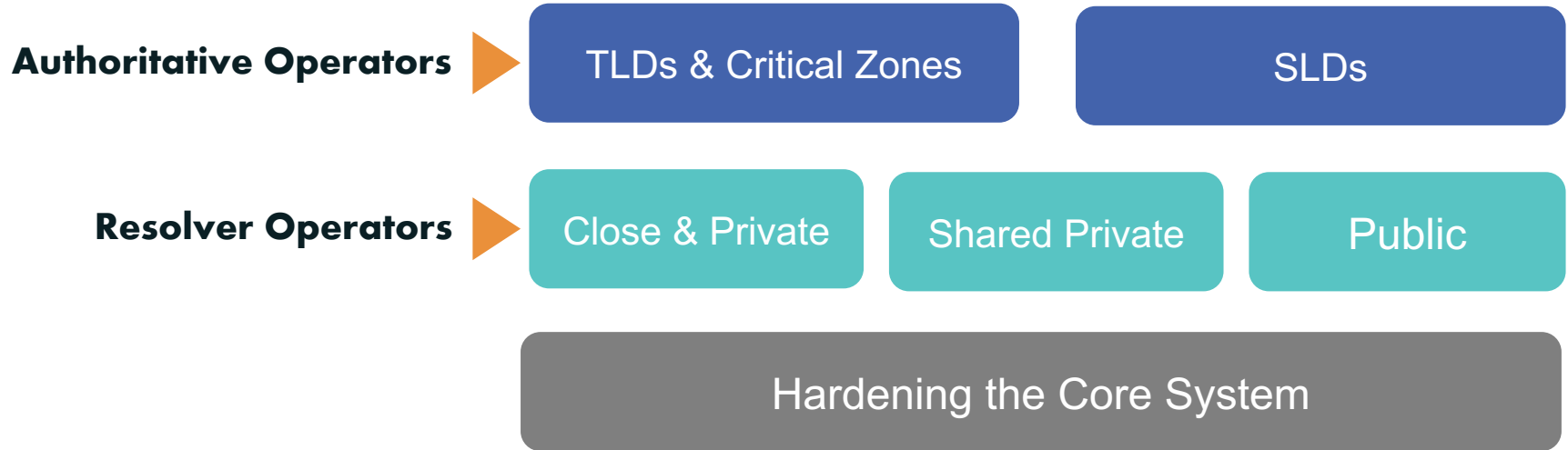
September 2022



An initiative supported by ICANN to produce 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.

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

..... is pronounced "kindness"



- 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.

For KINDNS purposes, the following are considered critical zones: Zones managed by Top-level Domain (TLD) operators/registries, including TLD zones themselves, Other delegation-centric zones of national importance for TLDs, SLDs tied to critical services such as healthcare and e-governance/citizen and ID services (e.g., mitid.dk), Finance/banking sites

TLDs & Critical Zones

1. **MUST** be DNSSEC signed and follow key management best practices.
2. Transfer 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

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. Transfer 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

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

Shared private resolver operators are typically ISPs or similar hosting service providers. They offer DNS resolution services to their customers (mobile, cable/DSL/fiber users, as well as hosted servers and applications).

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. 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 make up your DNS infrastructure **MUST** be monitored
7. **For privacy consideration:** Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

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

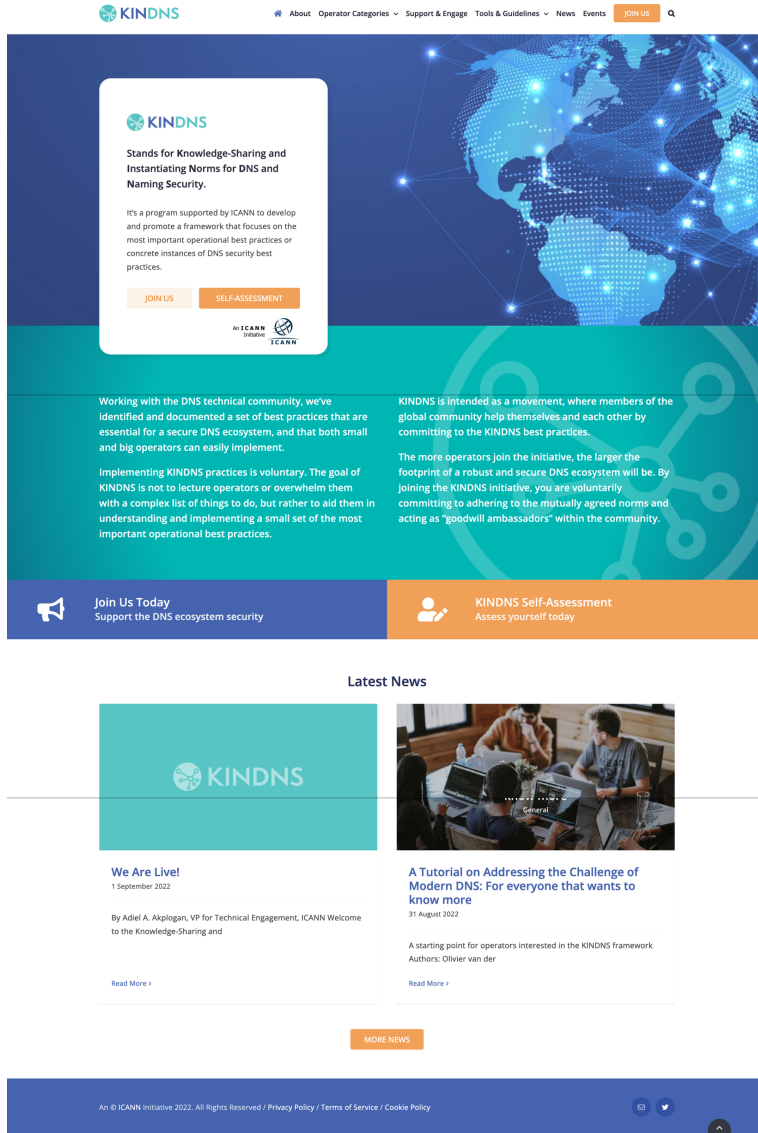
Shared Private resolvers

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

In addition to implementing best practices for DNS security and for DNS availability and resilience, all operators must pay careful attention to practices for hardening the platforms their DNS services use.

Core Hardening

1. ACLs **MUST** be implemented to control network traffic to your DNS servers
2. BCP38/MANRS egress filtering **MUST** be implemented
3. The configuration of each DNS server **MUST** be locked down
4. User permissions and application access to system resources **MUST** be limited
5. System and service configuration files **MUST** be versioned
6. Access to management services **MUST** be restricted
7. Access to the system console **MUST** be secured using cryptographic keys and/or two factor authentication mechanism.
8. Credentials Management for customer access **MUST** adhere to best practices



The screenshot shows the homepage of the KINDNS website. At the top, there is a navigation bar with the KINDNS logo on the left and a menu with items: About, Operator Categories, Support & Engage, Tools & Guidelines, News, Events, and a JOIN US button. Below the navigation bar is a large blue banner with a world map graphic. On the left side of the banner, there is a white box with the KINDNS logo and the text: "Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security." Below this text are two buttons: "JOIN US" and "SELF-ASSESSMENT". To the right of the banner, there is a paragraph of text: "Working with the DNS technical community, we've identified and documented a set of best practices that are essential for a secure DNS ecosystem, and that both small and big operators can easily implement." Below this is another paragraph: "Implementing KINDNS practices is voluntary. The goal of KINDNS is not to lecture operators or overwhelm them with a complex list of things to do, but rather to aid them in understanding and implementing a small set of the most important operational best practices." Below the banner is a section with two columns. The left column has a blue background and the text: "Join Us Today Support the DNS ecosystem security". The right column has an orange background and the text: "KINDNS Self-Assessment Assess yourself today". Below this is a "Latest News" section with two news items. The first item is titled "We Are Live!" and dated "1 September 2022". The second item is titled "A Tutorial on Addressing the Challenge of Modern DNS: For everyone that wants to know more" and dated "31 August 2022". Below the news items is a "MORE NEWS" button. At the bottom of the page, there is a footer with the text: "An © ICANN Initiative 2022. All Rights Reserved / Privacy Policy / Terms of Service / Cookie Policy".



1. Operators in each category can self assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices.
 - Self-Assessments is anonymous, and reports can be downloaded directly from the web site.
2. 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 becomes goodwill ambassadors and promote best practices.

KINDNS Self-Assessment-Final

All Results Dashboard

First response 06 September 2022 08:04 AM
 Last response 18 September 2022 02:03 AM

195

of 230 responses

32%

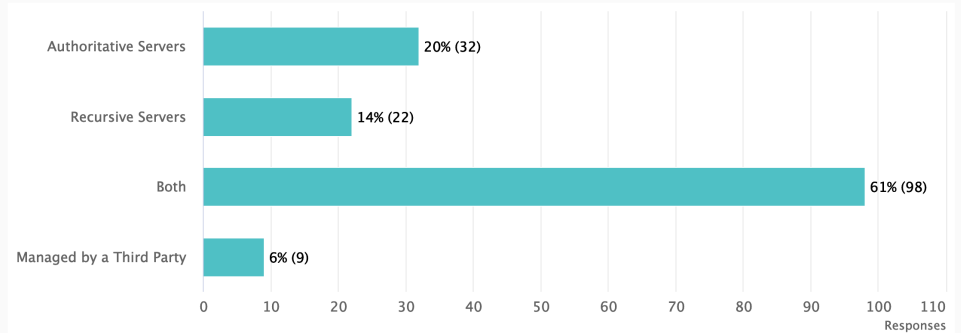
Completion Rate

03:20

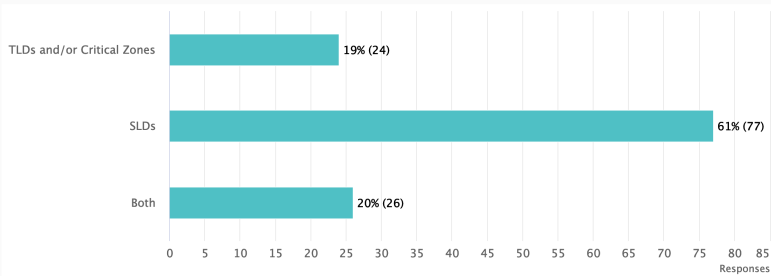
Minutes

Duration

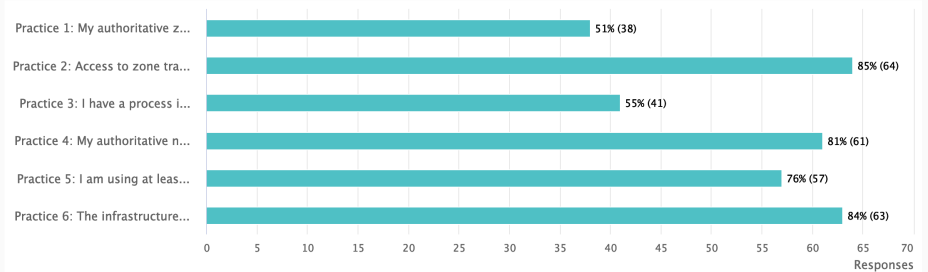
Part 1 Core DNS Operation Practices Assessment – Which component(s) of the DNS do you run?



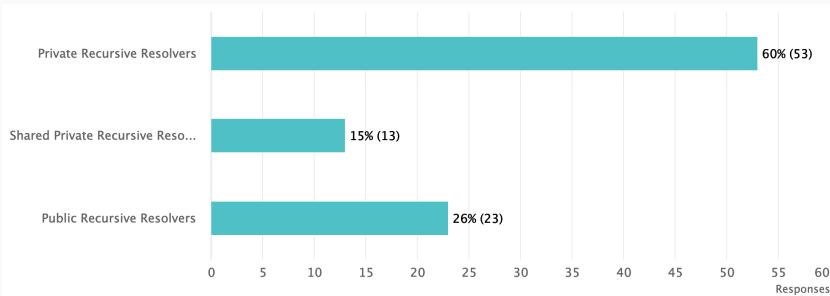
What Type of Authoritative Zone Do You Manage? – Type(s) of authoritative zone that you manage



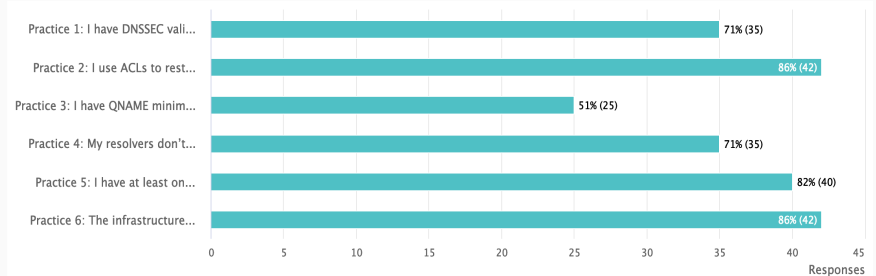
As operator of Authoritative Nameserver(s) for one or more Second Level Domains (SLDs), I implement and adhere to the following practices:



What type of Recursive Resolver do you run? – Type of recursion resolvers you run



As a Private Recursive Resolver operator, I implement and adhere to the following practices:



Website	www.kindns.org - launched on September 6 th
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Wiki page	https://community.icann.org/display/KINDNS <i>Where you can still find all the working documents.</i>
Mailing list	kindns-discuss@icann.org

Engage with ICANN



Thank You and Questions

Visit us at icann.org

Email: kindns-info@icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg