



KINDNS

KINDNS – Promoting DNS Operational Best Practices

Champika Wijayatunga
Regional Technical Engagement Manager - APAC
ICANN – Aug 8, 2022

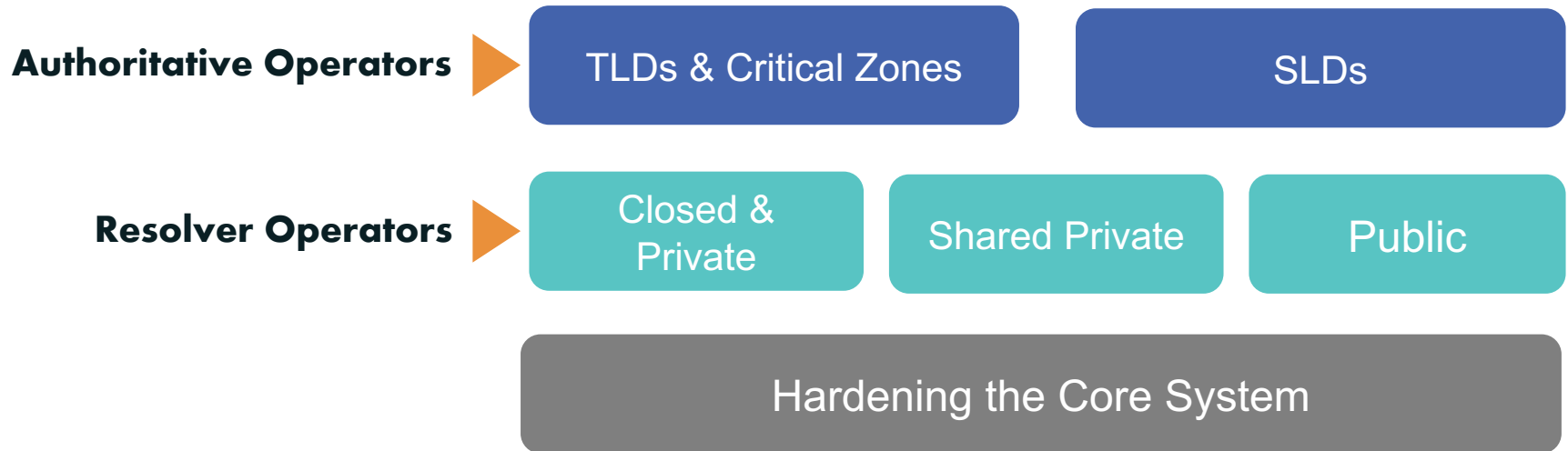


Knowledge-sharing and
Instantiating
Norms for
DNS (Domain Name System) and
Naming
Security

..... is pronounced "kindness."

An initiative to produce something simple to refer to 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 the industry identifies for better security and more effective DNS operations.

1. Identifying and documenting the most critical security norms for DNS operations (authoritative and recursive resolvers, and software)
 - Consulting and engaging with the operational community
2. Developing communications, promotions, and an enrollment plan
 - A dedicated information portal with best practices and implementation guidelines
 - Enroll DNS operators to participate and lead by example
3. Identifying indicators that will help measure and assess the impact of the initiative
4. Mapping best practices to ICANN DNS policy functions (Registry, Registrar, Registrant)



By joining the KINDNS initiative, DNS Operators are voluntarily committing to adhere to the identified practices and act as “goodwill ambassadors” within the community.

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 authoritative DNS software packages
7. Authoritative servers for a given zone **MUST** run from a diversified infrastructure
8. 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 a diversified infrastructure
7. The infrastructure that make 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. 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. Recursive servers **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 consideration: Encryption (DoH or DoT) **SHOULD** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. Data collected through passive logging of DNS queries **MUST** be limited
6. At least two distinct servers **MUST** be used for providing recursion services
7. Private resolver operators **SHOULD** have software diversity
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 a multi-factor authentication mechanism
8. Credentials for customer access **MUST** offer two-factor authentication

1. Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices
 - Self-Assessments will be anonymous, and a report can be directly downloaded from the web site
2. Operators can enroll to participate in one or many categories covered by KINDNS
 - Participation in KINDNS mean voluntarily committing to implement and adhere to agreed norms and practices
 - Participants becomes goodwill ambassadors and promote practices



- ⦿ **The KINDNS discussion mailing list:**

kindns-discuss@icann.org

- ⦿ **Wiki page** where we will share preliminary documents until the formal website is developed and launched

<https://community.icann.org/display/KINDNS>

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