red.es

DNS Information Guide

Version 1.1

Content

1. INTRODUCTION

Before delegating or changing the delegation of a DNS zone for domains under ".es" using the domain name management application accessible at the web address https://www.dominios.es/, it is advisable that the specified DNS servers are operational and accessible on the Internet, providing authoritative responses for the domain in question, and correctly configured in accordance with DNS technical standards in general and those outlined in this document in particular. Otherwise, the domain name may experience problems and may not be fully accessible on the Internet.

All DNS zones, both second and third-level, delegated under ".es," must be maintained and managed in a technically competent manner. This means that the DNS servers to which they are delegated must remain (as they were at the time of delegation) operational, accessible on the Internet, providing authoritative responses for the domain in question, and correctly configured in accordance with DNS technical standards in general and those outlined in this section in particular.

Any change affecting the delegation of a ".es" domain (registration, deregistration, or modification of the name or IP address of the DNS servers for the domain) must be planned and requested in advance and submitted to Red.es using the established procedure. In the event of technical incompetence or negligence, a DNS domain registered and delegated under ".es" may be temporarily or permanently deregistered.

red.es

2. CONFIGURATION REQUERIMENTS

1. To delegate a second-level DNS domain under ".es," it is necessary to have at least two authoritative DNS servers for the domain in question, or one authoritative DNS server and the secondary server for Dominios.es. It is recommended that there are more than two authoritative servers for the domain (up to a maximum of seven) and that they are physically in different networks and locations (for example, the primary server at the organization that owns the domain and a secondary server at the Internet service provider).

2. The names of the authoritative servers specified in the request must be the canonical names of said hosts (never aliases) and must match those indicated by NS records on the primary server for the zone in question. In the case of the primary server, the name must also match the name that appears as the source on the DNS server itself in the zone SOA.

3. All authoritative DNS servers for any second or third-level ".es" zone must be accessible from any point on the Internet in general, and from the primary ".es" server in particular (at least via TCP and UDP on port 53).

4. All authoritative DNS servers for any second and third-level ".es" zone must be providing authoritative and consistent responses for the zone in question.

5. All information contained within a ".es" domain (at any level) must be correct and have the necessary authorizations. Specifically, it is not permitted to place records of any type (NS, A, MX, CNAME, etc.), in any second or third-level DNS zone under ".es", pointing to computers external to the organization owning the domain in question without having express authorization to do so (this action could lead to the domain being taken down).

6. Lame delegations are prohibited in or under any second or third-level DNS zone under ".es". A lame delegation consists of placing an NS record for a domain or subdomain pointing to a computer that is not configured as an authoritative server for that zone. This action will be considered more

serious if the machine being pointed to incorrectly belongs to a third party outside the organization that owns the domain and could result in the domain being taken down.

7. The primary server of any second or third-level zone under ".es" must place glue records (type A records for authoritative servers in the zone) only for those servers under the domain associated with the zone and never for those external to it (such an action could result in the domain being taken down).

8. It is prohibited for an organization to configure a DNS server (even a cache-only DNS server) as forwarder pointing to an external server without explicit permission (such action could result in the domain being taken down).

9. An organization DNS clients must only point to internal DNS servers (or external ones with explicit permission).

10. The cache or root server file (usually named "named.root," "named.cache," or "named.ca") of every DNS server must always be updated with the latest version.

11. To help detect and resolve issues and inconsistencies between the primary and secondary servers, the recommended SOA serial number format for any DNS zone under ".es" (at any level) is as follows: **YYYYMMDDXX**. This is a 10-digit number, where:

    - YYYY = year of the last data modification in the zone
    - MM = month of the last data modification in the zone
    - DD = day of the month of the last data modification in the zone
    - XX = number of data modifications in the zone on the current day

    For example, the serial number 2025031203 in a SOA zone would correspond to the third SOA modification on March 12, 2025.

12. In order to maximize the "DNS traffic/DNS change propagation rate" ratio, the recommended standard values for SOA record parameters for second and third-level DNS zones under ".es" are as follows:

- SOA TTL = 3600 (1 hour)
- Refresh = 7200 (2 hours)
- Reetry = 3600 (1 hour)
- Expire = 2592000 (30 days)
- Minimum = 3600 (1 hour)

In special circumstances (for example, if significant or numerous changes are anticipated in the zone), the previous values for the TTL associated with the SOA record and the Refresh, Retry, and Minimum TTL times, may be temporarily lowered sufficiently, sufficiently in advance of the scheduled time for the changes so that the changes propagate on the Internet more quickly and reduce the cache time on the DNS Resolvers. It is important to note that the negative cache time that Resolvers will use for non-existent domain names will be the minimum of the TTL associated with the SOA record and the *Minimum* parameter specified in that record. In these cases, the recommended minimum values are as follows:

- SOA TTL = 900 (15 minutes)
- Refresh = 3600 (1 hour)
- Retry = 1800 (30 minutes)
- Expire = 2592000 (30 days)
- Minimum = 900 (15 minutes)

It is important that the notification and zone transfer mechanism on the primary and secondary servers work correctly. By using DNS Notifications, secondary servers can perform the zone transfer process immediately after receiving a notification, without having to wait for the Refresh time to expire.

13. It is recommended to configure support for incremental zone transfers (IXFR) to optimize bandwidth and transfer time. The first time a zone is transferred to a secondary server, it is fully transferred (AXFR). Depending on the volume of changes incorporated in the zone file update, the transfer may be AXFR even if IXFR is enabled.

14. If the ".es" domain server is acting as an optional secondary server for the second or third-level zone under ".es" in question, the minimum values for the SOA parameters mentioned in the previous section are not recommended but mandatory. In this case, setting Refresh, Retry and Minimum values lower than the mandatory minimums could result in the domain being deregistered.

15. The *mail address* field of the SOA for any second or third-level DNS zone under ".es" must always contain a valid email address (typically known as the hostmaster address) regularly operated by the technical contact person for the domain in question, who can be contacted if necessary. When specifying this address in the SOA for the zone, the "@" character must be replaced with the "." character (for example, "hostmaster.domain.es" to represent the email address "hostmaster@domain.es").

16. It is recommended that for all second and third-level domains under ".es", the email address "postmaster@domainname.es" exists and is regularly attended to by the person responsible for electronic messaging at the organization that owns the domain.

17. In order to provide security to the DNS service and prevent (among other things) spoofing attacks, the use of DNSSEC is recommended whenever possible. DNSSEC does not encrypt DNS responses, but adds signatures (RRSIG-type Resource Records) to the responses and, in case of no response (NXDOMAIN), it returns NSEC or NSEC3-type Resource Records that allow the validator to verify that the response is correct. In summary, the three security features provided by DNSSEC are:

    - Authentication of data origin
    - Data integrity
    - Proof of non-existence of data

    The first two functions are achieved with signatures (RRSIG) and the third with NSEC or NSEC3 records. DNSSEC uses asymmetric key encryption algorithms, typically generating two pair of keys: the KSK (Key Signing Key) and the ZSK (Zone Signing Key). Each pair of keys consists of a private key, which is used to generate the signatures, and a public key that will be used by validators (DNS Resolvers) to determine whether the responses are correct.

For **DNSSEC validation** performed by DNS Resolvers to be correct, the chain of trust must be complete throughout the entire DNS tree. All parent domains (in this case, the ".es" domain and the "." or "root" domain) must be signed, and each parent domain must contain the DS (Delegation Signer) record for the child domains. The DS record is a hash of the public KSK. DNS Validators will validate the public keys of all parent domains up to the root (trust anchor). In other words, each parent domain has a DS record in its zone file for each child domain that implements DNSSEC, allowing the chain of trust to be validated.

Before publishing the DS record in the parent domain (in this case, the ".es" domain registry), it is advisable to ensure that the public keys are correctly published in the DNS zone file and are correct. It is also advisable to verify that the signatures (RRSIG) and NSEC or NSEC3 records contained in the zone file are current and valid. When the DS record is published in the parent domain, the DNS Validators (Resolvers) will begin validating the responses.

3. FOR MORE INFORMATION

1. "DNS and BIND (4th. Edition)", P. Albitz y C. Liu, Ed. O`Reilly & Associates, ISBN 0-596- 00158-4, April 2001.

2. For a complete and up-to-date list of DNS-related RFC that may appear, please visit: https://www.rfc-editor.org/ y https://www.statdns.com/rfc/

3. ISC Presentations (Internet Systems Consortium): https://www.isc.org/presentations/

4. Guide to DNSSEC implementation and best practices (in Spanish): https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_guia_de_implantacion_y_buenas_practicas_de_dnssec.pdf