Version 14 July 2009

DNS check specifications

Introduction

These specifications relate to the DNS checks performed by SIDN's DNS Crawler. The DNS Report statement corresponding to each check is given in brackets; SIDN sends DNS reports to all registrars on a monthly basis.

Functional specifications

A test can trigger the following statements:

Critical: the delegation is 'lame'. SIDN reserves the right to delete the domain name from the .nl zone.

Error: the name servers definitely do not meet the technical requirements for .nl domain names; the noncompliance constitutes a (theoretical) threat to the stability of the internet and/or SIDN's name servers – due to unacceptably low TTLs, for example.

Warning: there are issues concerning the domain name: the name servers are not RFC-compliant and/or do not meet the technical requirements. However, the issues do not appear to constitute a threat to the stability of the internet and/or SIDN's name servers (although they may result in inconvenience for the registrant).

Notice: an irregularity has been detected, which is not very significant for the stability of SIDN's name servers or the contractibility of the domain name, but is inconsistent with the RFCs and/or the technical requirements. The irregularity might, for example, involve an extra name server associated with a 'child', which is not associated with its 'parent'.

Informational: extra information that is generated by the DNS check and logged, but does not influence the result.

IP addresses are checked for the following:

- Syntactic validity (ADDRESS:INVALID)
- RFC1918 status (ADDRESS:PRIVATE_IPV4)
- RFC3330 status (ADDRESS:RESERVED_IPV4)
- IPv6 special usage status (ADDRESS:RESERVED_IPV6)
- Association with a PTR record in the DNS (ADDRESS:PTR_NOT_FOUND)
- Existence of the host name that the PTR record points to (ADDRESS:PTR_HOSTNAME_NOT_FOUND)

Connectivity checks:

- A name server may not be announced by more than one AS (Autonomous System) number (IPv4 and IPv6 checks) (CONNECTIVITY:MULTIPLE_ASN).
- A name server must be announced by an AS number (CONNECTIVITY:NOT_ANNOUNCED).
- Domain name servers must be distributed across at least two AS numbers (CONNECTIVITY:TOO_FEW_ASN).

DNSSEC

- If the parent has a DS record, the child must support DNSSEC (DNSSEC:NO_DS_FOUND).
- If the child has a DNSKEY, the parent must have a DS-key (DNSSEC:DNSKEY_NOT_FOUND).
- The DNSKEY must not be of the type RSA/MD5 (DNSSEC:DS_ALGORITHM_MD5).
- At least one DNSKEY must be of the type RSA/SHA1 (DNSSEC:DS_MANDATORY_NOT_FOUND).
- The child may have a secure entry points (SEP) key (DNSSEC:DNSKEY_SEP).

- The RRSIG(DNSKEY) must be valid and must have been created by a valid DNSKEY (DNSSEC:DNSKEY_SIGNER_UNPUBLISHED).
- The RSSIG(SOA) must be valid and must have been created by a valid DNSKEY (DNSSEC:SOA_SIGNER_UNPUBLISHED).
- The DS must point to a DNSKEY that signs the child's RRset (DNSSEC:DS_KEYREF_INVALID).
- The DS may point to a SEP associated with the child (DNSSEC:DS_TO_NONSEP).
- At least one DS algorithm must be of the type RSA/SHA1 (DNSSEC:DS_MANDATORY_NOT_FOUND).
- Further DNSSEC processing must be verified (DNSSEC:CONSISTENT_SECURITY).

Delegation
- All name servers associated with the parent must also be associated with the child (DELEGATION:EXTRA_NS_PARENT etc.).
- Name servers associated with the child may also be associated with the parent (DELEGATION:EXTRA_NS_CHILD).
- At least two IPv4 name servers must be specified (DELEGATION:TOO_FEW_NS_IPV4).
- Where IPv6 is applicable to the name servers, at least two IPv6 name servers must be specified (DELEGATION:TOO_FEW_NS_IPV6).
- Glue should be consistent (DELEGATION:INCONSISTENT_GLUE).

Hosts
- Host names may contain only the letters a-z, the numbers 0-9 and the - character, RFC 952 (HOST:ILLEGAL_NAME).
- A host name must not end with a - character, but may begin with a number, RFC952 and RFC1123 (HOST:ILLEGAL_NAME).
- The host name's IPv4 or IPv6 address must exist in the DNS and must be resolvable (HOST:NOT_FOUND).
- A host name may not point to a CNAME (HOST:CNAME_FOUND).
- All IP addresses found, whether IPv4 or IPv6, must be valid IP addresses (ADDRESS:INVALID).
- A TLD may not be numeric, RFC3696 (HOST:ILLEGAL_NAME).[1]
  The length of a host name must not exceed a total of 255 octets, with no more than 63 octets per label, RFC2181 (HOST:ILLEGAL_NAME).

Mail
- The domain of the RNAME field should have a valid MX or A record (MAIL:DOMAIN_NOT_FOUND).
- An MX record for the domain name in the RNAME field must point to a valid host name (MAIL:HOST_ERROR).
- The mail exchanger must be contactable at least using IPv4 (MAIL:IPV6_ONLY).
- The e-mail address specified in the RNAME must be contactable using SMTP (SMTP:RECIPIENT_REJECTED).
- The zone should contain an SOA record (SOA:NOT_FOUND).
- There must not be more than one SOA record in the zone (SOA:MULTIPLE_SOA).
- The SOA record must have an MNAME that is a valid host name, as defined in the section headed 'Hosts' (SOA:MNAME_ERROR).
- The MNAME field does not have to be included in the list of NS records (and may therefore be a hidden primary, but this will result in the informational: SOA:MNAME_STEALTH).
- The server that is named in the MNAME field does not have to be contactable. However, if it is contactable, it must be an authoritative name server for the relevant domain (SOA:MNAME_NOT_AUTH).
- The syntax of the e-mail address in the RNAME field must be valid (SOA:RNAME_SYNTAX).

[1] Naturally, in our case, the TLD must always be .nl!

- The RNAME address must be deliverable (SOA:RNAME_UNDELIVERABLE).
- The SOA TTL value must be correct, i.e. at least 3600 seconds (SOA:MIN_TTL).
- The SOA refresh value must be at least 4 hours (SOA:MIN_REFRESH).
- The SOA retry value must lower than the SOA refresh value (SOA:RETRY_VS_REFRESH).
- The SOA retry value must be at least 3600 seconds (SOA:MIN_RETRY).
- The SOA expire value must at least 7 days (SOA:MIN_EXPIRE).
- The SOA expire value must be at least seven times as great as the SOA refresh value (SOA:EXPIRE_VS_REFRESH).
- The minimum SOA value must be less than 24 hours, but greater than 300 seconds (SOA:MINIMUM_SMALL and SOA:MINIMUM_LARGE).

Consistency

- The SOA serial numbers should be the same for all name servers (CONSISTENCY:SOA_SERIAL_DIFFERENT).
- The time-out values in the SOA records should be the same for all name servers (CONSISTENCY:SOA_DIGEST_CONSISTENT).

DNS

- The DNS check must establish whether EDNS0 is supported (DNS:NO_EDNS).

Name server

- The name server must have a valid host name, as determined by the checks under the heading ‘Hosts’ (NAME SERVER:HOST_ERROR).
- The DNS check must establish whether the name server is an open recursive resolver (NAME SERVER:RECURSIVE).
- Name servers must be authoritative (NAME SERVER:NOT_AUTH).
- Name servers must respond to UDP (NAME SERVER:NO_UDP_).
- Name servers must respond to TCP (NAME SERVER:NO_TCP).
- The DNS check must establish whether AXFR is possible (NAME SERVER:AXFR_OPEN).
- The DNS check must be capable of checking for version.bind, id.server and version.server (NAME SERVER:LEGACY_ID).
- In due course, it must also be possible to request the NSID (NAME SERVER:NSID).