Public-Root Name Server Operational Requirements

Published January the 17th, 2005

Status of this Document

This document provides information to the Public-Root and Internet technical community. This document specifies the formal recommendations and guidelines that define the standards applicable to the operations of the Public-Root name servers.

This document is a review of RFC2870 and its predecessor RFC2010. This document provides for enhanced security in the DNS through the deployment of intrusion detection systems. Furthermore, this Document provides for information privacy considerations as they apply to the data generated by root name servers.

This document is a work in progress. Contributions are welcomed, encouraged, and recognized. Distribution of this document is unlimited.

Abstract

The Internet is now critical to the world's social and economic infrastructure. The Internet community must be assured that the operation of this infrastructure is safe, reliable, and secure. The root domain name servers are a crucial part of this technology and infrastructure.

The primary focus of this document is to provide formal guidelines for the operation of root name servers. This document specifies operational requirements for root name servers including host hardware capacities, name server software, network connectivity, and physical environment.

The selection of name server locations, administrators, and the procedures for addressing noncompliance with these stated operational requirements are outside the scope of this document.

Other major zone server operators (gTLDs, ccTLDs, and large zones) may also find this document useful.

These guidelines are intended to meet perceived societal needs without overly prescribing technical details.

1. Definitions

For the purpose of this document the terms:

1.1 "AXFR" shall be used to refer to a specific command in the DNS protocol. AXFR is used to request the transfer of the entire zone between name servers.

1.2. "DNS" shall be used to refer to the Domain Name System protocol. The DNS helps users navigate the global Internet and connect their computers to web sites or other computers by translating domain names into valid Internet addresses.

1.3 "DNSSEC" shall be used to refer to DNS Security extensions. DNSEC adds security to the DNS protocol. It is a set of extensions that provide for origin authentication and integrity of data.

1.4 "GMT" shall be used to refer to Greenwich Mean Time.

1.5 "HIDS" shall be used to refer to a host based intrusion detection system.

1.6 The "IETF" shall be used to refer to the Internet Engineering Task Force. The IETF is a community of network designers, operators, vendors, and researchers concerned with the evolution and smooth operation of the Internet. The IETF is not a corporation and has no board of directors, no members, and no dues.

1.7 The "INAIC" shall be used to refer to The Internet Names Authorization & Information Center (INAIC). The INAIC is designated the administrative trustee of the content of the root (".") zone. The INAIC has final responsibility for the selection and correct operation of all of the zone's servers. The INAIC is also responsible for the operation of the Global TLD WHOIS database.

1.8 "LAN" shall be used to define a "Local Area Network". A LAN is a computer network that spans a relatively small area.

1.9 "MTBF" shall be used to define the mean time between failures of a device. This is the average time a device will function before failing. MTBF ratings are measured in hours.

1.10 "NIDS" shall be used to refer to a network based intrusion detection system.

1.11 "NTP" shall be used to refer to the Network Time Protocol. NTP is used to synchronize computer clock times in a network of computers.

1.12 The "PRSAC" shall be used to refer to the Public-Root Server Advisory Committee. The PRSAC shall give technical and operational advice to the Public-Root.

1.13 "PAR" shall be used to refer to Public Access Root name servers. PAR name servers provide direct resolution of the DNS to members of the general public and Internet community.

1.14 “Public-Root” shall be used to refer to the international federation of independent root operators that are responsible for the operation of the root name servers.

1.15 “RAR” shall be used to refer to Restricted Access Root name servers. RAR name servers only provide DNS support to Internet Service Providers.

1.16 “RFC” shall be used to refer to Request for Comments. RFC are publications of the IETF. Any submission to the IETF intended by the Contributor for publication as all or part of an IETF RFC is an "IETF Contribution". The INAIC and the PRSAC look to the IETF to provide engineering standards.

1.17 “TLD” shall mean top-level domain and refers to the suffix attached to Internet domain names.

1.18 “UDP” shall be used to refer to the User Datagram Protocol. UDP is a connectionless protocol that runs on top of IP networks. UDP is used primarily for broadcasting messages over a network.

1.19 “UPS” shall be used to refer to an uninterrupted power supply. This power supply includes a battery to maintain power in the event of a power outage.

1.20 “WHOIS” shall be used to refer to an Internet utility that returns information about a domain name or IP address. This utility provides access to directory service databases.

2. Background

The resolution of domain names on the Internet is critically dependent on the proper, safe, and secure operation of the root domain name servers. Public-Root name servers are provided and operated by a very competent and trusted group of professional volunteers.

2.1 The root name servers serve the root, also known as ".", zone. Today some of the root name servers also serve some TLDs (top level domains) although this is likely to change in the future.

2.2 The root name servers are neither involved with nor dependent upon the 'WHOIS' data.

2.3 The domain name system has proven to be sufficiently robust that we are confident that the temporary loss of most of the root name servers should not significantly affect operation of the Internet.

2.4 Experience has shown that the Internet is quite vulnerable to incorrect data in the root zone or TLDs. For this reason authentication, validation, and security of these data are of great concern.

3. The Servers

The following are requirements for the technical details of the root name servers themselves:

3.1 It would be short-sighted of this document to specify particular hardware, operating systems, or name serving software. Variations in these areas would actually add overall robustness.

3.2 Each server MUST run software which correctly implements the IETF standards for the DNS, currently [RFC1035] [RFC2181]. While there are no formal test suites for standards compliance, the maintainers of software used on root name servers are expected to take all reasonable actions to conform to the IETF's then current documented expectations.

3.3 At any time each server MUST be able to handle a load of requests for root data that is three times the measured peak of such requests on the most loaded server in then, current normal conditions. This is usually expressed in requests per second. This is intended to ensure continued operation of root services should two thirds of the servers be taken out of operation whether by intent, accident, or malice.

3.4 Each root name server SHOULD have sufficient connectivity to the Internet to support the bandwidth needs of the above requirement. Connectivity to the Internet SHOULD be as diverse as possible.

3.5 Root name servers SHOULD have mechanisms in place to accept IP connectivity to the root name server from any Internet provider delivering connectivity at their own cost.

3.6 RAR name servers MUST provide authoritative responses only from the zones they serve. The servers MUST disable recursive lookup, forwarding, or any other function that may allow them to provide cached answers. They also MUST NOT provide secondary service for any zones other than the root and associated zones. These restrictions help prevent undue load on the RAR name servers and reduce the chance of their caching incorrect data.

3.7 PAR name servers MUST provide responses to all zones. The servers MUST enable recursive lookup.

3.8 Root name servers MUST answer queries from any Internet host, i.e. MAY not block name resolution from any valid IP address, except in the case of queries causing operational problems. Problems that cause blocking SHOULD last only as long as the problem exists and be as specific as reasonably possible.

3.9 RAR name servers SHOULD NOT answer AXFR, or other zone transfer queries, from clients other than other root name servers. This restriction is intended to prevent unnecessary load on the root name servers.

3.10 PAR name servers MAY answer AXFR, or other zone transfer queries, from clients other than other root name servers. This provision is intended to allow members of the general public and Internet community direct access to the "." zone.

3.11 To avoid cache corruption the root name server SHOULD be a stealth secondary for the root zone.

3.12 The root name servers MAY put the root "." zone up for ftp, or other access, on one or more less critical servers.

3.13 Servers MUST generate checksums when sending UDP datagrams and MUST verify checksums when receiving UDP datagrams containing a non-zero checksum.

4. Security Considerations

The servers need both physical and protocol security as well as unambiguous authentication of their responses.

4.1 Physical security MUST be ensured in a manner expected of data centers critical to a major enterprise.

4.1.1 Whether or not the overall site in which a root name server is located has access control, the specific area in which the root name server is located MUST have positive access control. The number of individuals permitted access to the area MUST be limited, controlled, and recorded.

4.1.2 At a minimum control measures SHOULD be either mechanical or electronic locks. Physical security MAY be enhanced by the use of intrusion detection and motion sensors, multiple serial access points, security personnel, etc.

4.1.3 Unless there is documentable experience that the local power grid is more reliable than the MTBF of a UPS (i.e. five to ten years), power continuity for at least 48 hours MUST be assured. This MAY be accomplished through on-site batteries, on-site power generation, or some combination thereof. This MUST supply the server itself as well as the infrastructure necessary to connect the server to the Internet.

4.1.4 There MUST be procedures that ensure all power fallback mechanisms and supplies are tested no less frequently than the specifications and recommendations of the manufacturer.

4.1.5 Fire detection and/or retardation MUST be provided.

4.1.6 Provision MUST be made for rapid return to operation after a system outage. This SHOULD involve backup of systems software and configuration. It SHOULD also involve backup hardware that is pre-configured and ready to take over operation. This MAY require manual procedures.

4.2 Network security SHOULD be of the level provided for critical infrastructure of a major commercial enterprise.

4.2.1 The root name servers themselves MUST NOT provide services other than root name service. Remote Internet services and protocols such as http, telnet, rlogin, ftp, etc. MUST NOT be permitted on the root name servers.

4.2.2 The only login accounts permitted on the root name servers SHOULD be for the server administrator(s). "Root" or "privileged user" access MUST NOT be permitted except through an intermediate user account.

4.2.3 Servers MUST have a secure mechanism for remote administrative access and maintenance. Given the 24/7 support requirement (per section 5.5) there will be times when something breaks badly enough that senior technicians will have to connect remotely. Remote logins MUST be protected by a secure means that is strongly authenticated and encrypted. Sites from which remote login is allowed MUST be protected and hardened.

4.2.4 Root name servers SHOULD NOT trust other hosts except secondary servers trusting the primary server for matters of authentication, encryption keys, or other access or security information. If a root operator uses kerberos authentication to manage access to the root name server, then the associated kerberos key server MUST be protected with the same prudence as the root name server itself. This applies to all related services that are trusted in any manner.

4.2.5 The LAN segment(s) on which a root name server is homed MUST NOT also home crackable hosts. The LAN segments SHOULD be switched or routed so there is no possibility of masquerading. Some LAN switches aren't suitable for security purposes as there have been published attacks on their filtering. These can often be prevented by careful configuration and extreme prudence is RECOMMENDED. It is best if the LAN segment simply does not have any other hosts on it.

4.2.6 The LAN segment(s) on which a root name server is homed MUST be separately firewalled or packet filtered to discourage network access to any port other than those needed for name service.

4.2.7 The LAN segment(s) on which the root name server firewall is homed MUST be monitored by a network based intrusion detection system (NIDS). The NIDS MUST monitor all traffic in and out of the root name server firewall.

4.2.8 The root name server host MUST be monitored by a host based intrusion detection system (HIDS). The HIDS MUST monitor all traffic to the root name server.

4.2.9 All attempts at intrusion or other type of compromise SHOULD be logged. All the logs from all root name servers SHOULD be analyzed. This analysis SHOULD be conducted by a cooperative security team that communicates with all server operators to look for patterns, serious attempts, etc. Servers SHOULD log in GMT to facilitate log comparison.

4.2.10 Server logging SHOULD be to separate hosts that SHOULD be protected similarly to the root name servers themselves.

4.2.11 The server SHOULD be protected from attacks based on source routing. The server MUST NOT rely on address- or name-based authentication.

4.2.12 The network on which the server is homed SHOULD have in-addr.arpa service.

4.2.13 The root name servers SHOULD have their clocks synchronized via NTP [RFC1305] [RFC2030] or similar mechanisms in as secure manner as possible. For this purpose, servers and their associated firewalls SHOULD allow the root name servers to be NTP clients.

4.2.14 Root name servers MUST NOT act as NTP peers or servers.

4.3 Protocol authentication and security are REQUIRED to ensure that data presented by the root name servers are those created by those authorized to maintain the root zone data.

4.3.1 The root zone MUST be signed by the INAIC in accordance with DNSSEC, see [RFC2535] or its replacements. It is understood that DNSSEC is not yet deployable on some common platforms but that it will be deployed when supported.

4.3.2 Root name servers MUST be DNSSEC-capable so that queries MAY be authenticated by clients with security and authentication concerns. It is understood that DNSSEC is not yet deployable on some common platforms but will be deployed when supported.

4.3.3 Transfer of the root zone between root name servers MUST be authenticated and be as secure as reasonably possible. Out of band security validation of updates MUST be supported. Servers MUST use DNSSEC to authenticate root zones received from other servers. It is understood that DNSSEC is not yet deployable on some common platforms but that it will be deployed when supported.

4.3.4 A 'hidden primary' server, which only allows access by the authorized secondary root name servers, MAY be used.

4.3.5 Root zone updates SHOULD only progress after a number of heuristic checks designed to detect that erroneous updates have been passed. Human intervention MUST be requested in the event the update fails the tests.

4.3.6 Root zone updates SHOULD normally be effective no later than 6 hours from notification of the root name server operator.

4.3.7 A special procedure for emergency updates SHOULD be defined. Updates initiated by the emergency procedure SHOULD be made no later than 24 hours after notification.

4.3.8 In the event of a critical network failure each root name server MUST have a method to update the root zone data via a medium that is delivered through an alternative, non-network, path.

4.3.9 Each root MUST keep global statistics on the amount and types of queries received/answered on a daily basis. These statistics MUST be made available to PRSAC and PRSAC sponsored researchers to help determine how to better deploy these machines more efficiently across the Internet. Each root MAY collect data snapshots to help determine data points such as DNS query storms, significant implementation bugs, etc.

5. Communications

Communications and coordination between root name server operators, the Public-Root and INAIC are necessary.

5.1 Planned outages and other down times SHOULD be coordinated between root name server operators to ensure that a significant number of the root name servers are not all down at the same time. Pre-announcement of planned outages allows other operators to continue their normal operations.

5.2 Root name server operators SHOULD coordinate backup timing so that many servers are not off-line being backed up at the same time. Backups SHOULD be frequently transferred off site.

5.3 Root name server operators SHOULD exchange log files as they relate to security, loading, and other significant events. This MAY be handled through a central log coordination point or MAY be informal.

5.4 Statistics as they concern usage rates, loading, and resource utilization SHOULD be exchanged between operators and MUST be reported to the INAIC for planning and reporting purposes.

5.5 Root name server administrative personnel MUST be available to provide service 24 hours a day, 7 days per week. On call personnel MAY be used to provide this service outside of normal working hours.

5.6 The INAIC MUST maintain a database of root operators and said database MUST include the operators name and contact information.

6. Information Privacy Considerations

Legislation exists in many jurisdictions to provide for information privacy and consumer protection. These information privacy laws define how user data MAY be collected, for what purpose, and how it can be used.

6.1 Root name server operators MUST be familiar with local information privacy legislation, rules, and regulations affecting the transmission and collection of data.

6.2 Root name server operators MUST be familiar with the application of local law as it MAY apply to the generation, distribution, and retention of logs and statistical data.

6.3 In the event the root name server operator is unable to meet the provisions of section 4.3.9, then the root name server operator SHALL communicate those restrictions to PRSAC.

6.4 In the event the root name operator is unable to meet the provisions of section 4.3.9, then PRSAC SHALL make alternate arrangements for the analysis of the data subject to local privacy information legislation.

6.5 In the event the jurisdiction lacks privacy legislation, the root name server operator MUST ensure that any data represented by logs or statistical information remains strictly confidential.

7. References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC2010] Manning, B. and Vixie, P., “Operational Criteria for Root Name Servers”, RFC 2010, October 1996.

[RFC2030] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 2030, October 1996.

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC2535] Eastlake, D. and C. Kaufman, "Domain Name System Security Extensions", RFC 2535, March 1999.

[RFC2870] Bush, R., Karrenberg, D., Kosters, M., and Plzak R., “Root Name Server Operational Requirements”, RFC 2870, June 2000.

8. Specification of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

9. Full Copyright Statement

Copyright (C) The Internet Names Authorization & Information Center (2005). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Names Authorization & Information Center or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Names Authorization & Information Center or its successors or assigns.

This document and the information contained herein is provided on an **"AS IS"** basis and **THE INTERNET NAME AUTHORIZATION & INFORMATION CENTER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**