SAC117
Report on Root Service Early Warning Systems

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
13 July 2021

Preface

The Security and Stability Advisory Committee (SSAC) focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any dissenting opinions or alternative views that are included at the end of the document.

Table of Contents

Executive Summary

The SSAC reviewed many relevant publications on the topic of a root zone early warning system and provides a short summary of each in this report. The concept of an early warning system for the root zone comes originally from the Root Scaling Study Team and TNO Reports, both published in 2009. Since then the concept has evolved away from an original intention of modelling the potential impact on the operation of the root service with the addition of internationalized domain names (IDNs), IPv6, and new gTLDs to the root zone into a concept that is intended to provide feedback about the operational stability of the root service as more gTLDs are added to the root zone.

In reviewing these publications, the SSAC came to the conclusion that an early warning system for the root zone is currently infeasible, as was also concluded by OCTO-15. The root zone system is highly complex, and our current understanding of it does not allow us to predict imminent failure within its conventional and conservative operational parameters. This however, should not take away from efforts to better understand and gather data on the root server system, which root server operators are collecting, as described in RSSAC002[1] and RSSAC047.[2]

[1] See RSSAC002v4: RSSAC Advisory on Measurements of the Root Server System, https://www.icann.org/en/system/files/files/rssac-002-measurements-root-06jun16-en.pdf
[2] See RSSAC047: RSSAC Advisory on Metrics for the DNS Root Servers and the Root Server System, https://www.icann.org/en/system/files/files/rssac-047-12mar20-en.pdf

1 Background

In 2009 the ICANN Board asked the SSAC and RSSAC to study overall root stability[3] in the case of an increasing root zone size and other new technologies such as IPv6, DNSSEC and IDNs.[4] Two eventual outcomes of this request were the Scaling the Root Report,[5] and SAC046: Report of the Security and Stability Advisory Committee on Root Scaling.[6]

Recommendation #4 of SAC046 states:

> ICANN should update its "Plan for Enhancing Internet Security, Stability, and Resiliency," to include actual measurement, monitoring, and data sharing capability of root zone performance, in cooperation with RSSAC and other root zone management participants to define the specific measurements, monitoring, and data sharing framework.

As a response to this recommendation ICANN's Office of the Chief Technology Officer (OCTO) published OCTO-15: Recommendations for Early Warning for Root Zone Scaling.[7] OCTO-15 makes the argument that an Early Warning System (EWS) that could adequately predict failure due to root zone growth is largely infeasible because “none of the proposed measurements could be directly associated with scaling issues for the root zone,” and further internal measurements of the capacity of existing platforms that serve the root zone would require access to data that was proprietary to individual root server operators and potentially sensitive. It is also unclear whether any such measurements would expose intrinsic limitations or be remedied by upgrading the capacity of the root server system. Instead of building an EWS, OCTO-15 recommends, "… that the most reliable path forward is for periodic direct discussions with the groups that could be affected by root zone scaling issues."

The DNS records in the root zone and the root servers that serve it are dynamic and regularly changing. New technologies developed in the IETF and elsewhere have prompted evolutionary changes both to the content of the root zone and on the distribution of that content to resolvers. For example, the proposed addition of ZONEMD records to the root zone is a new technology that would alter the contents of the root zone.[8] Other technologies affecting distribution of the root zone content such as DNS over QUIC (DOQ),[9] Authoritative DNS-over-TLS (ADOT),[10] and

[3] Root stability can generally be defined as the continual ability of resolvers to query and receive correct responses for resource records in the root zone.
[4] See ICANN Board Minutes, February 3 2009, https://www.icann.org/resources/board-material/minutes-2009-02-03-en
[5] See Scaling the Root: Report on the Impact on the DNS Root System of Increasing the Size and Volatility of the Root Zone, https://www.icann.org/en/system/files/files/root-scaling-study-report-31aug09-en.pdf
[6] See SAC046: Report of the Security and Stability Advisory Committee on Root Scaling, dated 6 December 2010
[7] See OCTO-15: Recommendations for Early Warning for Root Zone Scaling, https://www.icann.org/octo-015-en.pdf
[8] See RZERC003: Adding Zone Data Protections to the Root Zone, https://www.icann.org/uploads/ckeditor/rzerc-003-en.pdf
[9] See draft-ietf-dprive-dnsoquic-02, Specification of DNS over Dedicated QUIC Connections, https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsoquic/02/
[10] See draft-ietf-dprive-unauth-to-authoritative-01, Recursive to Authoritative DNS with Unauthenticated Encryption, https://datatracker.ietf.org/doc/draft-ietf-dprive-unauth-to-authoritative/

hyperlocal root[11] may be integrated into the root service, and it is highly likely that these evolutionary developments will continue. Additionally, individual root server operators adapt their approaches to service delivery over time. For example, they regularly make changes to platform management, software diversity and network infrastructure. The deployment of such technologies may impact the long term stability of the root service, for better or for worse.

The SSAC convened a work party to review the findings of OCTO-15 in the light of previous studies on this topic. The work party reviewed published material and considered the feasibility, desirability and practicality of measuring root service performance with the intention of being able to identify early signs of stress in the delivery of the service, or, in other words, an "Early Warning System" for the root service.

This report uses terminology found in RSSAC026v2: RSSAC Lexicon in the manner prescribed in that advisory.[12] Where specific terminology is used that is not found in that advisory a definition is given.

This report uses the term *root zone system* (RZS) to refer to the entirety of administration, maintenance, publication, distribution, and serving of the root zone. The *root zone system* starts at the root zone administrator updating a record, ends at a root server instance responding to a query and encompasses everything in between.

2 Publication Review

This section is ordered chronologically by the date of each publication.

2.1 RSST Report

Published September 2009[13]

This report was published in 2009 by the Root Scaling Study Team (RSST), commissioned under the auspices of an ICANN Board action, where a steering group was formed from RSSAC, SSAC and ICANN Staff who developed a Terms of Reference for the study and engaged a team of subject matter experts to undertake the study. The report uses the terms *root system, root zone management process*, and *DNS root system* to refer to what this report calls the *root zone system*.

The study looked primarily at the process used to manage the distribution of the root zone and did not perform any data analysis on the performance of the root zone system.

[11] See RFC 8806: Running a Root Server Local to a Resolver, https://datatracker.ietf.org/doc/rfc8806/
[12] See RSSAC026v2: RSSAC Lexicon, https://www.icann.org/en/system/files/files/rssac-026-lexicon-12mar20-en.pdf
[13] See Scaling the Root: Report on the Impact on the DNS Root System of Increasing the Size and Volatility of the Root Zone, https://www.icann.org/en/system/files/files/root-scaling-study-report-31aug09-en.pdf

The report makes the case by analogy that the capacity of the RSS has a lead time in responding to changes in the service profile and advises that changes should be made at a pace that allows the various components of the service to adjust their operation to keep pace with the demands placed upon the service.

The report highlights the level of manual effort undertaken by various parties in this system, and notes the issues with the short term challenges of such a system to respond to abrupt increases in demand. However, there is no absolute scaling limit noted for the system.

The study included the development of a model of the RSS (See 2.2). This model noted that the system shows signs of stress when the root zone reaches 4,480 TLDs and becomes overloaded at 8,967 TLDs. It must be noted that these figures are a product of the model of the situation as of 2009, and some effort would be needed to assess to what extent this model is still applicable to the situation today or in the near term future.

There are two issues identified in this report:

1. The amount of checking that needs to be performed and the capacity of the root zone system to perform these steps. At some point scaling will overburden the amount of checking required, although the point of stress of such a system is indeterminate,
2. The size of a very large root zone calls into question the role of recursive resolvers and cache efficiency. There may be other technical capacity problems besides just the RSS.

This report was prepared before the IANA transition. At that time there was a higher processing overhead with the National Telecommunications and Information Administration (NTIA) of the United States Department of Commerce involved in root zone administration. Accordingly, it is not easy to relate these processes and the scaling numbers against the current situation as the model used in this study may no longer be relevant and the calculation of process capacity from the root zone system may not be directly applicable to the current situation.

Also, scaling the manual administration processes within the administration of the root zone system may be independent of more technically-based factors, such as scaling the distribution of updated root zones to root server instances. There might be a point where the manual processes cannot scale further and this may be the limiting factor.

2.2 TNO Report

Published September 2009[14]

TNO stands for *Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek*. In this report the term *TNO Report* is used as a shorthand for TNO's *Root Scaling Study: Description of the DNS Root Scaling Model*.

[14] See 2009 Root Scaling Study Description of the DNS Root Scaling Model, https://www.icann.org/en/system/files/files/root-scaling-model-description-29sep09-en.pdf

This is a report of a modeling contribution to the 2009 Scaling the Root study (See 2.1), focused on transforming the available information about the root zone system into a quantitative model and simulation software. No scalability analysis is given. Instead several numerical cases are simulated. The TNO Report uses the terms *DNS root server system, root server system, root zone management system*, and *root system* to refer to what this report calls the *root zone system*.

The purpose of the report is to describe its model, as a basis for:

- explanation of the quantitative root scalability model for the RSST and potentially other interested audiences,
- development of the quantitative simulation model by TNO.

Given the changes to the root zone since 2009, including the IANA transition, the introduction of DNSSEC, the increased use of anycast in root server operations, and the addition of IPv6 records, this report is largely outdated. Some aspects of the modelling approach may still be relevant. However, it is unclear how this modelling approach could be made applicable today.

2.3 SAC042

Published December 2009[15]

This report is SSAC's response to Board resolution 2009-02-03-04[16] that proposed to study the potential impact on the stability of the root zone and root server system when AAAA RRs, IDNs, DNSSEC, and more TLDs get added to the root zone. It is challenging to draw currently relevant conclusions from this SSAC commentary of the Root Scaling Study Team (RSST) and TNO Reports given how much has changed since 2009. Much of the focus of these studies was to address some concerns at the time arising from the deployment of IPv6, DNSSEC, IDNs, and new gTLDs in the root zone.

SAC042 uses the term *root zone management* and its acronym *RZM* to refer to what this report calls the *root zone system*. This should not be confused with the term *root zone maintainer (RZM)* from RSSAC026v2.

The report contains the SSAC's comments on the RSST Report, an interleaved response from the RSST, and in some cases a subsequent follow up from the SSAC on the response from the RSST. SAC042 contains no recommendations, nor does it have a findings section, but it does contain a formal record of a correspondence between the SSAC and the RSST.

It notes that the RSST model did not include detailed consideration of the Internet fabric (including caches) that intervenes between resolvers and root servers in their model. The SSAC highlighted the need to better understand the effects of scaling the root zone on resolver priming queries. The RSST explained why they recommended an early warning system instead of a

[15] See SSAC042: SSAC Comment on the Root Scaling Study Team Report and the TNO Report, https://www.icann.org/en/groups/ssac/documents/sac-042-en.pdf
[16] See ICANN Board Resolution 2009-02-03-04, https://www.icann.org/resources/board-material/minutes-2009-02-03-en

threshold prediction for root scaling. Their reasoning was, in part, because the human factors (manual modifying records at IANA) scale differently than machine factors (caches, queries/responses).

In response to a question from the SSAC on specific scaling factors the RSST responds:

> There is no meaningful quantitative answer to the question "what would happen to the root system if we added a million new TLDs?" because the system would start to evolve in both predictable and unpredictable ways as soon as the scaling process began, quickly invalidating whatever baseline had been used to construct the model.

The root zone early warning proposal was the outcome of the inability to define a threshold value or an algorithm that would generate a threshold value, and given this impossibility, the collective decision was to recommend an "early warning system". The RSST did not find a direct threshold that could be used to define a breaking point that would lead to some ill-defined but undesired outcome.

2.4 SAC046

Published December 2010[17]

This SSAC document notes that although the RSST delivered a report that embodied its best judgment in response to a broad set of questions, it did not accomplish the research specified in the Terms of Reference for the Study Team. It acknowledges that the allocated time, resources, and available data access was demonstrably inadequate to accomplish the requested work.

Following that effort, the RSSAC and SSAC also failed to converge on a common position and pursued separate responses to the Board of ICANN arising from the RSST report. SSAC046 is the SSAC's response to the Board's request in 2009-02-03-04.[18]

SSAC046 contains five recommendations:

1. Formalize and publicly document the interactions between ICANN and the root server operators with respect to root zone scaling. ICANN and the root server operators may choose to utilize RSSAC to facilitate this interaction
2. ICANN, National Telecommunications and Information Administration (NTIA), and VeriSign should publish statements, or a joint statement, that they are materially prepared for the proposed changes.
3. ICANN should publish estimates of expected and maximum growth rates of TLDs, including IDNs and their variants, and solicit public feedback on these estimates, with the end goal of being as transparent as possible about the justification for these estimates.

[17] See SAC046: Report of the Security and Stability Advisory Committee on Root Scaling, https://www.icann.org/en/groups/ssac/documents/sac-046-en.pdf
[18] See Draft Minutes of the Special Board Meeting, https://www.icann.org/resources/board-material/minutes-2009-02-03-en

4. ICANN should update its "Plan for Enhancing Internet Security, Stability, and Resiliency," to include actual measurement, monitoring, and data-sharing capability of root zone performance, in cooperation with RSSAC and other root zone management participants to define the specific measurements, monitoring, and data sharing framework.
5. ICANN should commission and incent interdisciplinary studies of security and stability implications from expanding the root zone more than an order of magnitude, particularly for enterprises and other user communities who may implement strong assumptions about the number of TLDs or use local TLDs that may conflict with future allocations.

The ongoing issues of Root Server Operator accountability and performance that are touched upon in this document have been taken up in more general terms in RSSAC037 and the Root Server Governance Working Group. The expectation, as captured in the Action Request Register, is that issues of root service performance and capacity to scale will be addressed after that activity has completed.[19]

As with the TNO Report (See 2.2) and SSAC042 (See 2.3), much has changed in the period since these recommendations were made.

2.5 SSAC Letter to the ICANN Board on New gTLDs

Published July 2012[20]

This is a 2012 letter from SSAC to the ICANN Board that states three concerns with the 2012 round of new gTLDs.

1. The SSAC did not believe a process for ordering applications bears upon the security and stability of the Internet.

2. The SSAC believed that questions regarding the maximum number of new TLDs that could be added to the root zone are misplaced. Instead, the proper concern was to ensure that the overall root zone publication system is audited and monitored to confirm that its resources can support an increase without degradation at the current service level.

3. Concerns raised in SAC042 and the TNO Report about combinatorial effects of adding IPv6, DNSSEC and new gTLDs to the root zone at the same time were no longer a concern since IPv6 and DNSSEC RRs had already been added to the root zone. The SSAC did not then believe the combinatorial issue was a concern.

This letter restated the five recommendations from SAC046 and noted that no progress had been made on them.

[19] See ICANN Action Request Register from March 2021, SAC046 R-4, https://www.icann.org/en/system/files/files/board-advice-status-report-pdf-31mar21-en.pdf
[20] See SSAC Letter to the ICANN Board on the New Generic Top Level Domain (gTLD) Process, https://www.icann.org/en/system/files/correspondence/faltstrom-to-icann-board-02jul12-en.pdf

2.6 SAC059

Published April 2013[21]

The ICANN Board asked the SSAC to clarify what it meant with SAC046, Recommendation 5. Specifically, the ICANN Board asked the SSAC to provide advice on how "interdisciplinary studies of security and stability implications from expanding the root zone more than an order of magnitude should be carried out and whom else should be consulted."

In SAC059 the SSAC advised that such a study be composed of experts from both DNS design and operational areas as well as being drawn from a broader set of expertise, including risk analysis and management, public policy, crime and law enforcement and intellectual property rights. The SSAC envisioned that this group would then explore both technical and non-technical concerns related to root zone expansion, including protocol and namespace issues, economic and business issues, abuse and law enforcement issues, and implications for end users.

The document notes in conclusion that:

> The SSAC believes that the community would benefit from further inquiry into lingering issues related to expansion of the root zone as a consequence of the new gTLD program. Specifically, the SSAC recommends those issues that previous public comment periods have suggested were inadequately explored as well as issues related to cross-functional interactions of the changes brought about by root zone growth should be examined. The SSAC believes the use of experts with experience outside of the fields on which the previous studies relied would provide useful additional perspective regarding stubbornly unresolved concerns about the longer-term management of the expanded root zone and related systems.

2.7 RSSAC022

Published October 2016[22]

This is RSSAC's single page response to the GNSO New gTLD Subsequent Procedures Policy Development Working Group, published in 2016.

The response noted that if future plans for more TLDs do not deviate from the previous expansion program then no technical issues are foreseen.

[21] See SAC059: SSAC Letter to the ICANN Board Regarding Interdisciplinary Studies, https://www.icann.org/en/system/files/files/sac-059-en.pdf

[22] See RSSAC022: Response to the GNSO Policy Development Process (PDP) Working Group on the new Generic Top Level Domains (gTLDs) Subsequent Procedures, https://www.icann.org/en/system/files/files/rssac-022-response-newgtld-06oct16-en.pdf

The response advocated a coordination program to allow changes to the root zone to be temporarily suspended if stress on the root service was observed by RSOs.

2.8 CDAR

Published March 2017[23]

Continuous Data-driven Analysis of Root Stability (CDAR) is a report, commissioned by ICANN, of an empirical study into the technical impact of the New gTLD Program on the security and stability of the root server system. The report uses the term *root DNS system* to refer to what RSSAC026v2 calls the *root server system*. The scope of CDAR is limited to what RSSAC026v2 calls the *root server system*, and does not cover what this report refers to as the *root zone system*.

There are two focus points for the report:

1. Did the delegation of additional gTLDs degrade the security or stability of the root server system?
2. Will further delegations degrade the stability or security of the root server system?

The data sets used for the analysis reported here are RSSAC002 data, DITL data and Atlas probe data.

The report concluded that:

- There was no measurable degradation of the stability or security of the root server system in the period until the writing of the report that could be attributed to the new gTLDs.
- There were no observed signs that the delegation of more new gTLDs in itself will degrade the stability or security of the root server system in the near future.

The report also speculated that the removal of new gTLDs from the root zone file could be a potential stability risk.

It was noted that the data sets for new gTLDs, as compared to the established TLDs, are very small, and the conclusions reached are impacted by this relative imbalance in the zone sizes and related query rates. The study did not include an analysis of recursive resolver query data to match the root server system data. It was not possible with this study to understand the relationship between queries seen at root server instances, and queries sent to recursive resolvers.

2.9 SAC100

Published December 2017[24]

[23] See Continuous Data-driven Analysis of Root Stability (CDAR), https://www.icann.org/en/system/files/files/cdar-root-stability-final-08mar17-en.pdf

[24] See SAC100: SSAC Response to the New gTLD Subsequent Procedures Policy Development Process Working Group Request Regarding Root Scaling, https://www.icann.org/en/system/files/files/sac-100-en.pdf

This document is the SSAC response to a question from the GNSO New gTLD Subsequent Procedures Policy Development Working Group on the subject of root zone scaling.

The SSAC makes several recommendations in this document including a recommendation for ICANN to continue its investigation into the general topic of early warning systems for the RSS as a whole, noting the distinctions between measurement of the service provided by individual root servers instances, measurement of services provided by individual RSOs, and measurement of the RSS as a whole.

The SSAC recommended a focus on the growth rate of the root zone rather than the absolute size of the root zone at any particular point in time, a response to any observed service instability by delaying further changes to the root zone, and for ICANN to investigate and catalog the long term operational factors of maintaining a larger root zone.

These recommendations were not addressed to the Board of ICANN, but to the co-chairs of the Policy Development Process Working Group on New gTLD Subsequent Procedures presumably for consideration for inclusion in the Working Group's report.

2.10 RSSAC031

Published February 2018[25]

This is RSSAC's response to the GNSO New gTLD Subsequent Procedures Policy Development Working Group. In this publication the RSSAC argues:

- An absolute cap on the number of new TLD delegations per-annum is the wrong way to think about root zone growth.
- The root zone should not grow more than 5% per-month. (i.e., use a shorter time period and use of a relative change metric, not absolute quantity). This strong recommendation is based on experience over the period 2014 - 2016.
- Root zone churn rate also matters. (i.e., a stable root zone with no changes is preferred to one that has constant alterations).
- Conservatism in root zone DNS resource record types is wise.
- A flatter name space may have implications for the root zone, though details of this argument are not provided in this document.
- The CDAR study (See 2.8) was based on a number of TLDs that were not themselves very popular in terms of query volumes. Without some notion of the level of use of TLDs the projections of what is safe in terms of numbers of new TLDs is a significant challenge.

The basis for this RSSAC response appears to be recent experience, arguing that if this was sustainable in the past there is a high probability that the system will continue to operate in a stable manner when the changes are within the parameters of previous experience.

[25] See RSSAC031: Response to the GNSO Policy Development Process (PDP) Working Group on the new Generic Top Level Domains (gTLDs) Subsequent Procedures, https://www.icann.org/en/system/files/files/rssac-031-02feb18-en.pdf

2.11 SAC103

Published October 2018[26]

This SSAC publication is in response to the GNSO New gTLD Subsequent Procedures Policy Development Working Group's initial report. It addresses various concerns, one of which is root zone scaling. This publication does not provide any further recommendations beyond those provided in SAC100. “The SSAC is pleased to see a preliminary recommendation from the working group calling for the ICANN organization to further develop root zone monitoring functionality and early warning systems, as it previously recommended [in SSAC 100]”.

2.12 RSSAC047

Published March 2020[27]

This document identifies an initial set of metrics for the Root Server System (RSS) as well as metrics for individual Root Server Operator (RSO) operations. The metrics for both contexts were developed with the idea that anyone who desired to examine the data used for the metrics could examine them and, if desired, develop their own collection and measurement system. The intent being that the data as well as it’s collection system would all be treated as open source.

The specific metrics and thresholds established for both the RSS and individual RSOs are for availability, response latency, correctness, and publication latency.

The document recognizes that the metrics and how they are calculated may change over time. An effort has been underway by the ICANN Office of the Chief Technology Officer (OCTO) to set up an initial implementation to gain operational experience with the metrics, their collection, and their utility.

The report recommends that ICANN commission an initial implementation of this measurement framework and use the experience to inform a prototype implementation of this measurement and collaborate with the Internet community to further refine these measurements over time.

This is not an early warning system per se, but the collection of current baseline performance measurements described in this report could be a central component in a technical set of service metrics for a baseline level of service for the RSS. Presumably the notion of service level failure could be marked by a deviation from this baseline service level.

[26] See SAC103: SSAC Response to the new gTLD Subsequent Procedures Policy Development Process Working Group Initial Report, https://www.icann.org/en/system/files/files/sac-103-en.pdf
[27] See RSSAC047: RSSAC Advisory on Metrics for the DNS Root Servers and the Root Server System, https://www.icann.org/en/system/files/files/rssac-047-12mar20-en.pdf

2.13 RSSAC002v4

Published March 2020[28]

The document defines measurements that all RSOs should implement for data gathering. RSSAC002 was originally published in 2014 and gets reviewed every two years; all RSOs currently provide RSSAC002 data.

The measurements include latency to publish available data from time of notification, traffic volumes, query and response size distributions, RCODE distribution and number of seen sources.

2.14 RSSAC052

Published November 2020[29]

This is RSSAC's comment on OCTO-15 v1: Recommendations for Early Warning for Root Zone Scaling. The RSSAC agrees with the assessment that there are no known, third party measurements that specifically detect scaling issues. Neither the metrics described in RSSAC002 nor those described in RSSAC047 explicitly address the detection of degradation of service due to scaling issues.

Scaling issues with respect to the rate of change are likely implementation-specific and difficult to predict within each RSO's infrastructure. The RSSAC recommends no significant change be made to the root zone that cannot be backed out on short notice. The RSSAC reiterates its advice from RSSAC022 and RSSAC031.

2.15 OCTO-15

Published February 2021[30]

The document makes the case that it is not feasible to predict the early onset of failure to serve the root zone caused by the number of entries in the root zone, or caused by the content of the root zone. It notes that while measurements may be feasible in relation to the specific technologies and platforms used by individual RSOs, any such measurement may be highly proprietary and not necessarily expose intrinsic limitations beyond capacity issues stemming from the specific platforms in use by RSOs.

---

[28] See RSSAC002v4: RSSAC Advisory on Measurements of the Root Server System version 4, https://www.icann.org/en/system/files/files/rssac-002-measurements-root-12mar20-en.pdf
[29] See RSSAC052: Statement on Recommendations for an Early Warning System for Root Zone Scaling, https://www.icann.org/en/system/files/files/rssac-052-25nov20-en.pdf
[30] See OCTO-15: Recommendations for Early Warning for Root Zone Scaling, https://www.icann.org/en/system/files/files/octo-015-01feb21-en.pdf

The document notes previous SSAC advice in SAC100 where SSAC recommended that ICANN should continue developing the monitoring and early warning capability with respect to root zone scaling.

The report notes that:

> There are apparently no measurements, whether made externally or reported by the RSOs themselves, that would reliably indicate issues with root scaling that a third party could detect. Instead, the RSOs can periodically report if they perceive any scaling issues. ICANN org can ask each individual RSO annually whether that RSO has experienced any issues related to root zone scaling, or if they anticipate any such issues based on their individual testing. Each RSO is in the best position to understand its own infrastructure and processes in order to report on scaling issues. In addition, the RSOs know that they can report at any time between requests, which should be sufficient for providing an early warning about effects on the RSS.

It further notes that monitoring RSSAC002 data would not allow an observer to predict root scaling issues. Instead individual RSOs are best suited to identify any scaling issues in their own infrastructure.

Regarding IANA's and ICANN's abilities to scale their processes in line with an expanding root zone, OCTO-15 notes that this topic is addressed by the review of IANA's Service Level Agreement (SLAs) via the Customer Standing Committee (CSC).

For the other stakeholders identified in the OCTO document (Recursive Resolver Operators, Anti-Abuse Communities) it notes that these communities can reach out to ICANN if they perceive any scaling issues, and ICANN can query groups in these communities if they perceive any scaling issues.

The report does not directly reference the RSSAC047 report on metrics for the root servers and the RSS (See 2.12). RSSAC047 defines: "measurements, metrics and thresholds that root service operators meet to define a minimum level of performance [..] which demonstrate that the root server system, as a whole is serving correctly and timely responses."

2.16 References to an Early Warning System for the Root Zone

In reviewing the published SSAC, RSSAC and other material on the topic of root service performance it is helpful to trace the specific references to this 'early warning' system for the root service within these documents.

The first reference to 'early warning' comes from the RSST Report (See 2.1). The RSST Report makes the case for an 'early warning system' as opposed to a 'threshold prediction' because: "[..] as the size, contents, and volatility of the root zone change, the important question for the community is dynamic and continuous, [..] not static and predictive." It's implied that this is the first use of 'early warning system' because the previous focus was on a 'threshold prediction'.

Additional evidence that the RSST Report provides the first discussion of an 'early warning system' can be found in the Root Scaling Study Terms of Reference.[31] This document set the terms of reference for the RSST Report and yet makes no mention of 'early warning'. However, it does ask numerous questions about quantities of entries in the root zone and their impact on stability.

From the Root Scaling Study Terms of Reference:

> As the number of entries increases, how will these numbers change? What are the capacities of the system? Where are the thresholds? Equally important to understanding the trends and limits is the need to identify mechanisms of avoiding expansion beyond limits that are considered to be operationally feasible. Are mechanisms in place to anticipate reaching these thresholds and to make adjustments? Are these realistic?

However, when outlining the expected deliverables of the RSST Report the Root Scaling Study Terms of Reference states:

> The study should not try to answer the question "how many entries in the root zone is too many?" but to show, as clearly and definitively and authoritatively as possible, what the consequences must be for each part of the system of changing the value of each variable.

Thus, while the Root Scaling Study Terms of Reference may have posed questions of quantitative thresholds, the expectation was that the RSST not limit itself to studying the impact of increasing quantities on the stability of the root zone system. This leeway facilitated the initial deployment of the term 'early warning system' in the eventual report of the RSST.

SAC042 (See 2.3) uses the term 'early warning system' in reference to the RSST Report, but it does not use the term independent of that. SAC046 (See 2.4) does not use the term. The SSAC Letter to the ICANN Board on New gTLDs (See 2.5) and SAC059 (See 2.6) do not include the term.

SAC100 (See 2.9) includes the term 'early warning'.

SAC100 recommendation 1 states: "ICANN should continue developing the monitoring and early warning capability with respect to root zone scaling." Then cites the RSST Report: "root system oversight should focus on 'early warning' rather than threshold prediction. [..] The focus of root zone management policy should be the establishment of effective mechanisms for detecting and mitigating risks as they become visible."

Later in the explanatory text of SAC100 recommendation 1 the term is used again:

> The CDAR study also recommends a set of "risk parameters" that they believe are worth monitoring. These are: (i) multiple .com-sized gTLDs, (ii) post-retirement and pre-delegation traffic, and (iii) an increase in server-side processing on the root DNS

[31] See Root Scaling Study Terms of Reference, https://www.icann.org/resources/pages/root-scaling-study-tor-2009-05-05-en

> system. The SSAC recommends ICANN consider including this list as a set of parameters to be part of the early warning system.

The explanatory text for SAC100 recommendation 2 again uses the term in a quote from the RSST Report.

In RSSAC031 (See 2.10) the RSSAC advises that: “The ICANN organization should, in consultation with the community, coordinate further efforts among the root zone management partners and the root server operators to develop an early warning system for the Root Server System as an aggregate, in order to ensure we have the ability to detect issues as early as possible.”

Finally, in SAC103 (See 2.11) the SSAC voiced its approval for the GNSO New gTLD Subsequent Procedures Policy Development Working Group calling for an ‘early warning system’: "The SSAC is pleased to see a preliminary recommendation from the working group calling for the ICANN organization to further develop root zone monitoring functionality and early warning systems, as it previously recommended.”

3 SSAC Comments

The general intentions of early warning systems are to instrument a system such that signs of imminent failure will be detected before the system being observed actually fails.[32]

The United Nations International Strategy for Disaster Reduction defines *early warning system*:[33]

> The set of capacities needed to generate and disseminate timely and meaningful warning information to enable individuals, communities and organizations threatened by a hazard to prepare and to act appropriately and in sufficient time to reduce the possibility of harm or loss.

Early warning systems tend to rely on an observed correlation between an observed event or conditions and an ensuing event. They are conventionally predicated on a number of assumptions. These include:

- System failure is not a sudden event without warning, but the development of an extended process that has one or more trigger events that have a high risk of causing the failure outcome or are correlated with the ensuing outcome.
- Failure modes are predictable. There is a distinction between a change in the operational behaviour of a system that is within the range of acceptable system behaviours and a change that creates an operational behaviour that is regarded as a failure. If we do not understand the nature of what could be regarded as normal operation, it is very challenging to define thresholds of behaviours that can be regarded as failure.

[32] See Early warning system models and components in emergency and disaster: a systematic literature review protocol, https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-019-1211-5
[33] See UNISDR Terminology on Disaster Risk Reduction (2009), https://www.undp.org/content/dam/georgia/docs/publications/GE_isdr_terminology_2009_eng.pdf

- Failure is an adverse event or situation that lies outside the conventional operational parameters of the system and lies outside the parameters of events that can be mediated or avoided by operational responses.

In constructing an early warning system, it is useful to understand the operational parameters that encompass normal (or non-failing) modes of system behaviour, and also useful to understand the tolerance of the system to change. When designing an early warning system that will warn of a heightened risk of impending systemic failure, it is necessary to identify the changes to the operational behaviour of the system that presage further changes that lie outside of the system's normal tolerances.

It is noted that novel systems, where there is not a rich history of operational experience, are more prone to unanticipated events; without a history of operational experience these events may trigger a failure situation. It is also noted that highly complex systems may experience emergent behaviours. Charles Perrow argues in *Normal Accidents* that multiple and unexpected failures are built into complex and tightly coupled systems. Thus, operational accidents are unavoidable and cannot be designed around.[34] In such systems, the assumptions underpinning the viability of monitoring the system for early signs of impending failure may not be valid.

If the implicit question being posed by an early warning system for the root zone is what is a threshold number of entries in the root zone that would be infeasible for the RZS to support, then this is a question that does not have a well understood answer in any case.

The range of possible answers start at a highly conservative stance that the current root zone is operationally viable and any larger zone has not been proven to be operationally viable, so any change over and above the current zone size could be seen as an early warning of a heightened risk of operational failure. A different answer observes that there are extremely large zones in operation in the DNS, and the service provided by these zones appears to be acceptable to users, so any root zone size less than what already exists in other zones would represent no heightened level of risk to the root zone system. Aside from a relatively subjective quantification of risk, there is no evidence in any of the material reviewed that would objectively distinguish between these cases in terms of heightened risk to the root service. This is consistent with the observation that efforts to identify a threshold size of the root zone that would present unacceptable risk to the root zone system have not achieved any clear consensus.

In the absence of a plausible threshold value as to what constituted an unacceptable risk, the approach used was one of cautious exploration. With this approach the current state is considered to be within the bounds of acceptable risk, future changes applied to the system are moderate relative to the existing size and state of the system and the behaviours of the system are carefully monitored. If at any point the measurements show some form of degradation of the system's performance, the change process can be halted and the system state can be further analysed.

However, this approach has to be reconciled with the assertion made in OCTO-15 that: "There are apparently no measurements, whether made externally or reported by the RSOs themselves, that would reliably indicate issues with root scaling that a third party could detect." This assertion has to be placed into a relative context. It is assumed that this comment is not referring

[34] See Perrow, Charles. "Normal Accidents: Living with High Risk Technologies" New York: Basic Books, 1984.

to a sudden change in the root zone to hold a further billion or so new TLDs. Such a sudden and substantial change would in all likelihood lead to operational issues with the root zone system.

However, if the rate of change is capped by both the number of changes in any update and the size of each update, then there is an expectation that the root zone system would adapt in ways that would result in relatively constant acceptable behavior, and it is in this context that the OCTO-15 comment is appropriately interpreted.

The evident practical challenges in instrumenting the root zone system to provide early warning signs of service impairment or even failure do not apply to the more general task of measuring the RSS. The SSAC notes the utility of the RSAAC002 data in informing other studies of the root service, such as the 2017 CDAR analysis (See 2.8). The current efforts in establishing a baseline current service level performance measurements, described in RSSAC047 are also seen as very useful in providing a solid foundation of service performance data that can be used to ground future studies of the evolution of the root zone system, and are seen to be a valuable addition to the public data relating to the root server system. Accordingly, the SSAC continues to support the advice provided in both RSSAC031 (See 2.10) and RSSAC052 (See 2.14).

It is useful to note a distinction between this focused examination of the root service, the root zone system, and the broader issues of stability and robustness of the DNS itself. This report has looked at the implications for the root zone system, and its operations, in the context of growth and evolution of the root zone. It has reflected on the feasibility to instrument the root zone system to warn of signs of impending stress that would lead to the likely failure of this system.

This report does not look at the implications of any such changes on the broader DNS system, and how the broader DNS system could be monitored for emergence of stress points and potential failure of part of this larger system. In short, this report is not intended to be interpreted as a comment on the feasibility, or infeasibility, of an early warning framework for the DNS itself. That is, necessarily, a distinct topic of study that is not considered here.

4 Conclusion

The SSAC reviewed many relevant publications on the topic of a root zone early warning system and provides a short summary of each in this report. The concept of an early warning system for the root zone comes originally from the Root Scaling Study Team and TNO Reports, both published in 2009. Since then the concept has evolved away from an original intention of modelling the potential impact on the operation of the root service with the addition of internationalized domain names (IDNs), IPv6, and new gTLDs to the root zone into a concept that is intended to provide feedback about the operational stability of the root service as more gTLDs are added to the root zone.

In reviewing these publications the SSAC came to the conclusion that an early warning system for the root zone is currently infeasible, as was also concluded by OCTO-15. The root zone system is highly complex, and our current understanding of it does not allow us to predict imminent failure within its conventional and conservative operational parameters. This however,

should not take away from efforts to better understand and gather data on the root server system, which root server operators are collecting, as described in RSSAC002 and RSSAC047.

However, the lack of an early warning system for the root service or the determination that deploying one is currently not feasible should not be interpreted as meaning that the root service is currently at risk of imminent failure. The operational history of the system as a whole has demonstrated high stability through various modes of growth. The SSAC has not identified any reason to expect that sudden failures will occur if future growth in the system continues at a rate similar to that observed in the past. However, continued vigilance on the operational state of the root zone system is a prudent operational measure, and in this context the measurement and analysis of performance of the root server system is an important ongoing activity.

5 Acknowledgments, Statements of Interest, Dissents and Alternative Views, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members and outside experts who contributed directly to this particular document, as well as ICANN org staff who facilitated the work. The Statements of Interest section points to the biographies of all SSAC members and invited guests, which disclose any interests that might represent a conflict—-real, apparent, or potential—-with a member's or invited guest's participation in the preparation of this Report. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any dissenting opinions or alternative views.[35]

The Dissents and Alternative Views section provides a place for those individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have withdrawn and recused themselves from discussion at any stage during the development of this report. Except for members listed in the Dissents and Alternative Views and the Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

5.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Comment.

SSAC members
Joe Abley
Jaap Akkerhuis
Tim April

[35] See SSAC Operational Procedures v9.0, Section 1.1, https://www.icann.org/en/system/files/files/ssac-operational-procedures-v9.0-05jan20-en.pdf

Patrik Fältström
James Galvin
Julie Hammer
Geoff Huston
Warren Kumari
Russ Mundy
Rod Rasmussen
Matthew Thomas
Suzanne Woolf

ICANN staff
Andrew McConachie (editor)
Danielle Rutherford
Kathy Schnitt
Steve Sheng

5.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2021-01-07-en

5.3 Dissents and Alternative Views

There were no dissents or alternative views.

5.4 Withdrawals

There were no withdrawals.