NEW gTLD Program

SUMMARY REPORT AND ANALYSIS OF PUBLIC COMMENT – Term of Reference for the Root Scaling Study

EXECUTIVE SUMMARY

- A memo was published for the ICANN community's comment on 5 May 2009 setting the terms of reference for the scaling study.
- A scaling study has been conducted by a select study team to inform the SSAC and RSSAC report to the Board on this issue. (http://www.icann.org/en/announcements/announcement-2-18sep09-en.htm).
- An additional report from the Steering Group to the ICANN Board is being prepared which will include the findings of this study as well as other conclusions and recommendations to the Board from RSSAC and SSAC.

Sources

Public comments postings (29 May to 31 July 2009), the full text of which may be found at http://forum.icann.org/lists/scaling/.

COMMENT SUMMARY

Support for the terms of reference for the Root Scaling Study as proposed. The At-Large Community welcomes and strongly supports the terms of reference for the Root Scaling Study as proposed. This excellent document clearly identifies the issues at stake. The At-Large Community looks forward to the findings and the model that will be suggested by this expert team. *ALAC (31 July 2009).*

Size and Capacity of Root Zone. Today's root zone is small enough to make it practical for caches to regularly and efficiently fetch compressed and digitally signed copies out of band (e.g. using HTTP, rsync, or BitTorrent). Caches that do so benefit from improved DNS resolution efficiency while also lessening load and dependence on central network infrastructure. Whatever policies ICANN adopts for adding new records to the root zone should maintain this property. The growth of the root zone file (in bytes) over time should try to stay within Moore's law. This seems as reasonable as any estimate about the capacity of caches to handle a complete local copy of the root zone. *M. Dempsky (22 June 2009).*

Isn't it true that increasing the frequency of updates, and the size of the root zone file, would make it much harder to have benefits from caching of the entire zone file locally? If the entire root zone file is 68KB, it might in the future be treated like the hints file. Stability (through a small root zone file, rarely changing) would be enhanced if the number of TLDs is small, in other words. *G. Kirikos (29 May 2009).*

Costs and technical effects of increasing zone file. Aren't there costs that the team is not anticipating if the zone file is increased to huge levels (e.g. 68MB, instead of 68KB today or even smaller with compression)? For example, if the zone file was tiny and only changing a couple of times per day, it is conceivable that one day satellites that transmit signals for the Global Positioning System (GPS) worldwide could transmit root zone updates through a low bandwidth (in other words, cheap) part of the spectrum on a continuous basis, worldwide to all devices. Systems such as this would be "out of band" and provide an extra level of resilience to the entire global Internet that is increasingly important to world economies. Increasing the size of the root zone might make such a system infeasible or too costly. *G. Kirikos (29 May 2009).*

Design and Long-Term Impact. Isn't it true that all else being equal a parsimonious design is best in the long-run? In other words, your "tests" need to be robust not just for today's problems, but for things you've not even thought about or imagined. *G. Kirikos (29 May 2009).*

Adding more root servers. There has been a longstanding political issue with the historical requirement of having only 13 name servers in the hints file, most of which are under the direct or indirect control of the U.S. government. It has been a subject of discussions both inside the ICANN community and outside (WSIS/IGF). Since the research of this study will examine among other things what would happen if the hints file grows larger due to DNSSEC signing (and more IPv6 records), it may be useful to see if adding more root servers would be possible without destabilizing the DNS as a whole. There may be no technical need to increase the number of root servers. Still, if

we could address the political issue at the same time, this would be welcomed by some parts of the Internet community. *P. Vande Walle (29 June 2009)*.

Questions for ICANN staff related to root server system root scaling study (submitted by G. Kirikos):

One of the most important concerns of those commenting on the new gTLD process has been the continued security of the DNS system. These questions submitted to ICANN appear to be within the group's terms of references:

(1) Zone File Changes and new gTLDs. IANA currently appears to be involved in zone file changes (see these pages, last updated in 2002-2003: http://www.iana.org/procedures/nameserver-change-requests.html; http://www.iana.org/procedures/nameserver-change-procedures.html)
. (a) While they specify ccTLDs explicitly, do those procedures apply to gTLDs currently?
(b) Are those the proposed procedures going forward if any new gTLDs are to be added to the root?

(2) IANA and ICANN--Resources and Workload. According to the ICANN Dashboard, in the past two years IANA has "root zone requests" of roughly 20 to 30 per MONTH on average (say 1 per day). According to the latest dot-com registry monthly report at page 7 (http://www.icann.org/en/tlds/monthly-reports/com-net/verisign-200812.pdf) Table 6.2 records that the total monthly nameserver write transactions alone were 2.49 million for December 2008, which is roughly 2% of all domains. More alarming is that 37.5 million "modify" transactions took place (Table 6.1) which corresponds to more than 40% of all domains, on average, during the month.
(a) In a world of thousands or tens of thousands of new gTLDs, where ICANN has limited experience acting as a registrar or registry (save for their management of the root for roughly 200 top-level domains), can the procedures in Question 1 above scale to handle the increased workload?
(b) What are the anticipated resources that will be needed to handle the increasing number of incoming requests? In particular, will the quality of service decline for existing gTLDs if IANA faces an increased workload due to newbie gTLDs?
(c) Some more detailed stats from IANA might be helpful to break down their workload either by gTLD or by the age of the registry operator to determine whether newer gTLD operators cause a disproportionate level of work.

(3) U.S. Department of Commerce Resources and Workload with new gTLDs. The U.S. Department of Commerce receives submissions for root zone changes (according to sections 7 and 8 -- http://www.iana.org/procedures/nameserver-change-procedures.html).
(a) Does this mean that the U.S. Department of Commerce can reject the addition of any new gTLDs into the root (even if ICANN or IANA approve them)?
(b) Given the U.S. Department of Commerce is on record opposing new gTLDs, and in light of the increased workload discussed in item #2 that would be expected, has the U.S. Department of Commerce costed out what additional resources they will need to keep up with an increased workload?

(4) "Glue Records". The use of "glue records" could pose some security and/or economic (free riding) issues. Example: if I am the owner of example.com I can go to my registrar and create a glue record for a malevolent nameserver named "subdomain.example.com" and point it to any IP address of my choice, say 123.45.67.89. That glue record is then added to the dot-com zone file. If I own a very high traffic website, say example2.com, I can have all the media files for its embedded content placed on a server at the IP address 123.45.67.89 (say http://123.45.67.89/image.gif) but which can now be accessed at http://subdomain.example.com/image.gif. Because the IP address corresponding to that malevolent subdomain appears directly in the zone file for .com, the request is handled by VeriSign (manage of the .com zone file), and not by example.com's own name servers (if it even has any real ones).

(a) Is this understanding of glue records correct, that I can offload all DNS requests directly to the registry operator above me through carefully picking which subdomain I use?
(b) More creatively, can a malevolent individual pick glue records corresponding to www.example.com (or other popular subdomains) and offload the vast majority of their DNS requests to the zone manager above them (think for example content delivery handled by special domains like Yahoo's yimg.com for instance, which handles all their image files)?
(c) Given (a) and (b) wouldn't a gTLD operator be able to have glue records added to offload DNS requests directly to the root zone operators, thereby "free riding" on the root zone operators?
(d)With DNS queries costing $1 per 1,000 requests – (see overage pricing—http://www.ultradns.net/index.php?fuseaction=order): isn't it possible that there could be economic strain imposed on root server operators if their loads increased substantially (even without glue records being abused)?

(5) Potential malevolent attacks; security audit.
(a) What's to stop a malevolent gTLD operator from adding a glue record for www.google.com or www.citibank.com into the root zone and diverting all the traffic from the victims to an IP address of their choice?
(b) To answer (a) it appears that step (6) of:
http://www.iana.org/procedures/nameserver-change-procedures.html
would help thwart that kind of attack; however, if those checks failed (e.g. if procedures became fully automated), or were thwarted by DNS cache poisoning or BGP hijacking targeted at IANA, wouldn't it be possible for security of the root to be overturned?
(c) Given the importance of the root zone file, especially for the U.S. government (.gov) and the military (.mil), shouldn't any new program be thoroughly reviewed by security experts (including those from the U.S. military) so that exposure to all potential new vulnerabilities is minimized?
(d) Would it be fair to say that increasing the number of agents and gTLDs that have access to introduce changes to the root zone file increases the probability that human error will manifest itself in a security breach? In other words, if the root zone is smaller, isn't it more secure?
(e) Would it be fair to say that given some potential gTLD operators have operated in grey areas of ICANN policy in the past (e.g. domain tasting,

registration of hundreds of phantom/clone registrars to increase threads in domain drops or land rushes, etc.) that those same actors will not hesitate to exploit any loopholes in IANA management procedures for the root zone for their own economic benefit, to the detriment of others?
(f) Given ICANN/IANA has not revised IANA root zone file change procedures in 6 or 7 years (see question 1), would it not be fair to say that a security audit by experts is essential to ensure that the potential for commercial exploitation of any grey areas in policy is eliminated before any new gTLDs are added?

G. Kirikos (29 May 2009).

ANALYSIS

With resolution 2009-02-03-04, the ICANN Board asked the Root Server System Advisory Committee (RSSAC), the Security and Stability Advisory Committee (SSAC), and the ICANN staff to study the potential impact on the root zone stability that might arise when IPv6 address records, IDN top level names, other new TLDs, and new records to support DNS security are added to the root zone. The Board expressed interest in hearing of the impact of the distinct changes, but also their aggregate effect on root zone operations. The Board also asked that the study address the technical and operational concerns regarding expanding the DNS root zone that have been expressed on this topic. In response to the Board's request, the three groups formed a steering group and organized a focused study. A memo was published for the ICANN community on 5 May 2009 setting the terms of reference for the study.

A comment forum was opened to allow the community to direct the steering group towards particular issues of concern involved in the study or the root scaling issues. Below is a summary of comments received during the comment period.

Since this time, a study has been conducted by a select study team and posted to the ICANN website: (http://www.icann.org/en/announcements/announcement-2-18sep09-en.htm). This study answers most of the questions raised during the comment period.

An additional report from the Steering Group to the ICANN Board is being prepared which will include the findings of this study as well as other conclusions and recommendations to the Board from RSSAC and SSAC.

As part ICANN's ongoing efforts to ensure the stability of the DNS, ICANN also contracted with the DNS Operations, Analysis and Research Center (https://www.dns-oarc.net/) as independent and well-respected experts to provide an analysis of the impact of adding IPv6, DNSSEC, and additional top-level domains to the ICANN-operated L root server (http://www.icann.org/en/announcements/announcement-17sep09-en.htm.) This report will also inform the Steering Group report.

The report of the Root Scaling Study Team commissioned by the Joint SSAC/RSSAC/Staff Steering Group addresses many of the issues raised by the respondents.

In particular, the report reviewed the current process used by ICANN/IANA, NTIA, and VeriSign's root zone group in processing change requests for the root zone; identified key manual processes that will still be applicable when change request processing is more fully automated; and determined that the technical checks performed by IANA and VeriSign in processing those requests make malicious changes refered to in the comments extraordinarily difficult to put into effect. That is to say, that certain checks in processing glue request steps will remain in process regardless of volume and this should alleviate concerns that malicious requests will be inadvertently accommodated.

The concerns noted by George Kirikos regarding glue records is not valid for changes in the root zone as it is outside of procedure for one TLD to designate a nameserver for a second TLD without both parties agreeing.

Additionally, while there are some specific instances of unique consideration for some ccTLDs in processing change requests, the process for adding or modifying root zone data (name servers and/or glue records) is the same for both ccTLDs and gTLDs. ICANN is engaged in documenting this process more fully for TLD managers as part of the ccTLD IDN fast-track project and this documentation will be shared with the community upon completion.

ICANN resources in management of the root zone change request process are one element studied in the RSST report. Their finding was that while resources can expand appropriately through the normal budget and planning process, at a certain point (greater than 3000 TLDs) the burden of the manual processing steps would exhaust ICANN's ability to manage the process without adding additional automation and mechanical checks. Root zone growth is projected to be 300-600 (gTLD and IDN ccTLD) over the next 30 months (i.e., most of that growth will occur in 2011 but there will not be additional growth until 2112). It is planned that the next phase of IANA automation will occur in time to meet the ceilings described in the report. It is well recognized though, that a thorough operational analysis for IANA and other ICANN functions is necessary to address all levels of growth. The growth of any service requirements resulting from a two or three times multiplication of the root zone is significant and will be challenging to manage. This would remove key elements of the process that allow ICANN/IANA staff to ensure that a concatenation of changes to one TLD do not result in an unofficial change in management of the TLD, such as a "stealth redelegation." Similar considerations exist for the manual elements of the NTIA authorization process and VeriSign's manual checks in their production of the root zone twice daily. Finding appropriate solutions for this limit point of productivity will be a key element in accommodating a growing root zone.

Questions regarding the size of the root zone and capacity of the root server operators (RSOs) to manage distribution of the zone, make up another significant element of the RSST report. Again, the findings of the RSST were that the RSOs are able to accommodate significant increases in root zone size, and with sufficient budget and planning time can keep abreast of the growing needs for an expanded root zone.

Another key finding of the RSST was that to enable the best possible practices in management of the root server system, all of the parties –ICANN, NTIA, VeriSign, and the root server operators – must share planning responsibilities, and develop metrics to

determine if the system is coming under stress (an early warning system) so that responses to that stress come into being in a timely and productive fashion.

RESPONDENTS

Peter Bartram
Nevil Brownlee
Matthew Dempsky (M. Dempsky)
George Kirikos (G. Kirikos)
Bill Oxley
Patrick Vande Walle (P. Vande Walle)
At Large Advisory Committee (ALAC)