Registry Stakeholder Group Discussion Group on Registry Service Providers

Summary of discussions

Date: February, 9 2018

Purpose

The Registry Service Provider Discussion Group (RSP DG) was formed to discuss: (i) streamlining migration of registries between back-end registry service providers (RSPs), (ii) improvements to operational SLA issues, and (iii) providing the Subsequent Procedures Working Group (Sub Pro WG) with insight into the experience of current RSPs.

Background

For many new gTLDs launched during the 2012 round of the New gTLD Program, as well as some "legacy" gTLDs, certain technical and other functions of the gTLD registry are performed by an independent contractor to the Registry Operator (RO). These contractors, known as Registry Service Providers (RSPs) or "back-end" providers, usually provide registry services around the five critical functions of a domain name registry, listed below. Such services are intended to provide key functional components to the RO and enabling the RO to meet Service Level Agreement (SLA) obligations required under their Registry Agreement (RA) with ICANN.

1. DNS
2. DNSSEC
3. Whois/RDDS
4. EPP
5. Data Escrow

In some cases, more than one RSP can provide services to a single RO. For example, some ROs may select one RSP to provide EPP and RDDS services and one or more different DNS service providers. It is critical to bear in mind that, in an ecosystem of over 1,200 new gTLDs, there are many different business models for both ROs and their relationships with RSPs. Any solutions or recommendations to improve trust in the operations and technology must recognize and allow for these differences as well as support future innovations.

To ensure that each new gTLD applicant had the technical capability to operate a new gTLD in a secure manner, the New gTLD Program included requirements designed to test the capability of ROs and their third-party service providers to address security, stability and resiliency requirements, known as Pre-Delegation Testing (PDT).

- **Testing**. PDT was conducted in a staged environment prior to delegation of each gTLD and prior to commencement of production operations. It was required to ensure that an applicant had the capacity to operate a new gTLD in a stable, secure manner. The testing that was conducted was broad and was conducted 1,200 times; the same test was performed for each gTLD, regardless of whether multiple gTLDs were operated by the same RO or shared the same RSP.

- **Emergency Back End Operators (EBEROs).** In the interest of protecting registrants and ensuring that delegated new gTLDs are sure to be stable, secure and resilient, ICANN created emergency thresholds for the five critical registry functions outlined above. An RO's failure to operate its new gTLD within these thresholds may provide ICANN with the option to trigger deployment of an EBERO, which would effectively require the transfer of the technical operation of the gTLD to an ICANN selected EBERO provider.

- **ICANN Monitoring.** ICANN monitors service performance against SLA's including some of the five critical functions listed above and detailed in Spec 10 of the RA. It is the understanding of the RSP DG that ICANN intends to roll out additional monitoring of RO performance to SLAs in 2018.

ICANN Data on the Current Registry Operator's Systems

During the Madrid DNS Symposium / ICANN GDD Summit in May 2017 as well as the ICANN 59 meeting in Johannesburg in June 2017, ICANN provided information about potential SLA violations that took place from 2014 through 2016. On August 31, 2017, ICANN updated that data with the most current set of measurements. The data shared by ICANN shows that there have been 32 cases where a gTLD reached one of the emergency thresholds:

  - 16 out of 32 cases were triggered by perceived failures in the DNS/DNSSEC services,
  - 16 out of 32 cases were triggered by failures in the RDDS service.
- Of the 32 cases, 10 occurred prior to the TLD's Sunrise period, 8 during Sunrise, 5 before general availability, and 9 during general availability.
- 11 RSPs, 26 gTLDs and a total of 211.7k active names, were involved in the 32 cases.
- The root cause, which ICANN began tracking in 2015, can be broken down as follows:
  - RDDS:
    - 3 were due to IPv6 transport failure;
    - 1 was caused by a broken chain of trust in DNSSEC; and
    - 1 was due to the web WHOIS service not responding.
    - For 11 of these RDDS cases, ICANN does not know the root cause as the cases occurred before ICANN began documenting the causes of each incident.
  - DNS/DNSSEC:
    - 5 cases exhibited issues in which either the DNS servers were not responding or if they were responding, they were returning a malformed DNSSEC response where the NSEC3 records were not included;
    - 2 cases were caused by expired signatures followed by breakage of the chain of trust in DNSSEC;
    - 2 cases arose when there was no response from the DNS servers (apparently a routing issue);

- 1 case of expired DNSSEC signatures;
- 1 break in the chain of trust in DNSSEC; and
- 1 case where there were no DS records when requesting delegation from IANA.
- 4 of these cases occurred in 2014, for which ICANN does not know the root cause.

Scope of the Discussions

The scope of these discussions relates to RSP operations for the new gTLDs that were established through the 2012 New gTLD Application round. Here, we are primarily focused on areas for potential improvement in the ongoing operation of such TLDs and the migration of registry services between RSPs. The concept of RSP accreditation has been raised and is one topic of discussion within the Subsequent Procedures PDP WG (Work Track 1).

1) Initial PDT. The PDT testing conducted by ICANN for every gTLD was designed to ensure that RO's were technically capable - prior to launch - of providing registry services in-line with the SLAs contained in the RA. Certainly, testing new RSP capabilities is a necessary and welcome endeavor to ensure the security and stability of platforms. That said, RSPs supporting a portfolio of TLDs that were essentially identical found the repetitive testing to be illogical and unnecessarily burdensome. It is not clear from the data provided by ICANN that testing an RSP multiple times increased the stability of TLD operation or provided any other tangible benefit. Prior to the next round, thought should be given to designing a single PDT that could better ensure that RO's (directly or through their chosen RSP) will meet the technical specification at launch and moreover, that they will be able to operate the live TLD or TLDs within the minimum requirements of the RA. Potential areas for improvement to the testing may involve positive success conditions around:
    a. DNS Management,
    b. DNSSEC operations;
    c. RDDS; and
    d. IPv6.

    The RSP DG notes that PDT, in whatever form or frequency, is by its nature a test intended to scope the preparedness of a Registry Operator to provide services at any given point in time, usually prior to launch of the gTLD. This type of testing is important to ensure that ROs are equipped to operate a gTLD, but understandably cannot fully prevent future SLA incidents.

    The RSP DG is of multiple minds regarding an accreditation or competency program. Some members would welcome a way in which ROs could be deemed sufficiently tested and stable to provide registry services for TLDs that may be migrated to their system without additional scrutiny. On the other hand, some members do not believe such a program would provide meaningful improvements to security or stability of the system and have concerns regarding the additional contractual and regulatory burden such a system may create.

2) Ongoing Monitoring and Reporting. As evidenced by the data presented by ICANN, there has been no guarantee that pre-testing of an RSP will result in *full* SLA compliance or guard against future SLA failures. PDT was designed to test against functional specifications rather than SLA's. Rather than focusing simply on pre-approval, solutions that ensure ongoing SLA compliance, such as increased

and transparent monitoring, should be explored. Since the launch of the latest round, ICANN has rolled out various monitoring of RSP services. The results of ICANN's monitoring should be made available to the ROs as anonymized/aggregated data for all TLDs collectively, and individually for the RO's own TLDs. Instances of SLA failure should be treated ubiquitously without discrimination as each case permits.

ICANN should continue to report regularly to the community about SLA failures that occur, particularly those that breach the emergency threshold and would trigger EBERO. It should do so in a manner that does not violate the confidentiality obligations owed towards ROs by anonymizing and/or aggregating data. The RSP DG appreciates the data it has already been provided to date and would request that, in addition to monitoring and reporting SLA failures that occur, ICANN should also conduct an analysis of the root cause of the failures in each instance and report those findings as appropriate. Such transparency is critical for the community to continue to develop recommendations to further enhance the security, stability and resiliency of new gTLDs and the DNS.

3) gTLD Migration Between ROs. Currently, ICANN uses PDT to assess the technical capabilities of gaining ROs prior to approving the migration of a gTLD between ROs. It is our understanding that this test was designed for gTLDs that have not yet launched in order to test ROs that are using RSPs that do not have any gTLDs running successfully on their platforms. Some members of the RSP DG support the development of a leaner test specifically designed with the migration of a delegated gTLD in mind. An alternative to this approach is some kind of pre-approval, as is being considered by the Sub Pro WG, with which a gTLD could migrate to without the requirement of additional testing is favored by some members of the RSP DG. In this instance, history of SLA performance could act as a measure of the RSP's capabilities particularly once SRS monitoring is effective. Incentivizing RSPs to maintain higher levels of service to become pre-approved in this manner could enhance security and stability, while also potentially making gTLD migrations less burdensome and safe.

4) EBERO. Despite SLA violations that have reached emergency thresholds, only in one instance has ICANN transitioned a gTLD registry to an EBERO (.WED[1]). While ICANN has not publicly stated why it has refrained from using the EBERO mechanism, ICANN has indicated to the Sub Pro WG that in each case where the emergency thresholds were reached, it was their determination that the transition of that registry to an EBERO would have incurred more risk, time and resources than allowing the impacted RO to resolve the underlying issues. While it may be worth maintaining the EBERO system to be invoked in extreme cases of registry failure, the EBERO system is potentially too costly a solution when the market seems to be in a position to provide a more cost-effective alternative. In addition, a different solution to address individual SLA failures is something ICANN could consider. For example, in instances of DNS failure, having an emergency DNS provider that ICANN could rely on if RSP DNS services fails. Such an emergency DNS provider could initially try to get a fresh zonefile and keep synchronized with the failing RSP DNS to the extent possible, in order for such an event to cause the minimum friction and disruption. The RSP DG notes that ROs for new gTLDs are required to maintain Business Continuity Plans, which if properly executed, ought to address this concern.

5) RSPs' Relationship with ICANN. There has been discussion as to whether or not RSPs should have a direct contractual relationship with ICANN in order to ease the lines of technical communication.

[1] https://www.icann.org/news/announcement-2017-12-08-en

While some ROs support this type of arrangement, other ROs prefer that all communication with ICANN flow through them. While introducing a formal RSP-ICANN relationship may improve the flow of information between ICANN's SLA monitoring staff and its compliance staff to respond to SLA failures more quickly, introducing a formal relationship between a third-party RSP and ICANN may create additional operational burdens for ICANN and ROs without guaranteed improvements to performance against SLAs or the avoidance of SLA failures. There is little to suggest that such a relationship would meaningfully improve the security, stability and resiliency of RSP operations. As independent contractors, RSPs are financially incentivized to maintain a high level of performance, or else risk losing the business of the ROs for whom they provide registry services. That said, it is feasible for any RO to give permission for ICANN to have direct contact with their chosen RSP and it is practical that a standard form of such permission be developed. The development of such a standard permission has wide support in the DG. The RSP DG notes that ICANN should continue to hold ROs directly accountable for the performance of their registry services, regardless of whether they perform those services themselves or through a contract with an RSP.

6) Next Round. For the next round, some of the RSP DG supports the recognition of a pool of RSPs that are currently and successfully providing registry services, in the belief that real life historical performance better reflects the ability to deliver service than any amount of PDTing can. Others in the RSP DG do not support a "grandfathering" type arrangement where past performance would automatically green light an RSP for future gTLD rounds. Should RSPs be given some kind of formal ICANN recognition in the next round of applications, a thorough review of their SLA performance should be conducted and taken into consideration, perhaps a 12-month look back. If RSPs are given recognition by ICANN, the question of who shoulders the responsibility in case of any subsequent performance failure would then also need to be considered. Under a direct contractual relationship between ICANN and an RO that does not name a specific RSP, as is the current situation, then the responsibility for any performance failure rests clearly and squarely with the RO.