Query by Proxy Approach for Pre-Delegation Testing

{V. 1.1; 2 May 2013}

Background

The security issues of providing the unicast IP addresses of DNS anycast instances has been noted by ICANN and these issues has been carefully considered while designing the procedures for the Pre-Delegation Testing (PDT). The primary objectives for direct instance queries are:

- Verify DNS protocol compliance (e.g. authoritative answer, DNSSEC processing)
- Verify zone propagation delay (for compliance with the registry agreement)

It should be noted that query performance and/or query latency measurements are not an objective for direct instance queries. These are handled by applicant self-certification and/or by ICANN performing on-site auditing of load testing (as stated in the Applicant Guidebook).

Even though the Pre-Delegation Testing Provider executes its services under a strict non-disclosure agreement with ICANN, ICANN recognizes that there are providers who may be unable to allow even limited test traffic to the unicast addresses of their DNS anycast instances ("direct instance queries").

Introduction to Query by Proxy

To address the issues with direct instance queries, Pre-Delegation Testing allows for query-by-proxy as an alternative to direct instances queries. This effectively means that the Pre-Delegation Testing Provider will send direct instance queries to a proxy operated by the DNS service provider. The proxy will forward the queries to the anycast instances and relay the reply back to the testing provider.

Query-by-proxy eliminates the need for the Pre-Delegation Testing Provider to communicate directly with each DNS anycast instance. For additional security, queries to the proxy may be filtered and/or rate limited, if required by the DNS service provider.

Input Data & Terminology

Input data should follow the XML schema provided for the DNS test. These templates can be found within the PDT System Data Submission Templates, under the Pre-Delegation Testing Resources section of the Pre-Delegation Testing page. http://newgtlds.icann.org/en/applicants/pdt

A **zone** is delegated to one or more **name servers**, each having one or more **public addresses** indended for use by clients on the Internet.

A single name server may be provisioned as an **anycast cluster** served by instances at different topological and/or geographical dispersed **locations**. Each **location** will be tested as part of the Pre-Delegation Testing (PDT).

A single location may be served by multiple physical nodes, to which traffic is distributed locally. The PDT does not aim to test each physical node at a single location -- only one node per location will be tested.

For each location that is to be queried, the following information is required:

- A numerical *location id_* that must be unique within a single cluster.
- A *query target* used to determine where to send queries for the location (see below).
- An optional *proxy flag* indicating that the communication is relayed via proxy.
- An optional *location description*.

Query Target

The **query target** may be specified as:

- An IPv4/IPv6 address.
- A FQDN (*Full Qualified Domain Name*) used for SRV/AAAA/A-based query lookup, in that priority order.

Unless an explicit port number is given - either as a query target attribute or as part of an SRV lookup - queries will be sent to port 53.

If the target is given using a FQDN, an SRV record using the following parameters will be performed to determine where to send queries. If an SRV record cannot be found, lookup will fall back to the AAAA record of the FQDN. If that also fails, a A record will be queried for.

- service=_domain
- proto=_tcp or proto=_udp (depending on DNS query to be performed)

Example 1: Send a UDP DNS query to target *ams1.proxy.example.com*:

1. Look up SRV for *_domain._udp.ams1.proxy.example.com*.
2. Send query to server/port specified by SRV record using UDP transport.
3. If SRV record cannot be found, look up AAAA record for *ams1.proxy.example.com* and send query using UDP transport to port 53.
4. If AAAA record cannot be found, look up A record for *ams1.proxy.example.com* and send query using UDP transport to port 53.

Example 2: Send a TCP DNS query to target *ams1.proxy.example.com*:

1. Look up SRV for _domain._udp.ams1.proxy.example.com.
2. Send query to server/port specified by SRV record using TCP transport.
3. If SRV record cannot be found, look up AAAA record for *ams1.proxy.example.com* and send query using TCP transport to port 53.
4. If AAAA record cannot be found, look up A record for *ams1.proxy.example.com* and send query using TCP transport to port 53.

Example 3: Send a UDP DNS query to target "192.0.2.42":

1. Send query to 192.0.2.42 port 53 using UDP transport.

DNS Proxy Requirements

The following requirements apply to a DNS proxy used to relay queries to remote name servers:

- The DNS proxy MUST NOT modify any relayed DNS query and/or response.
- The DNS proxy MAY filter incoming queries based on source address and/or rate-limit incoming queries to 100 queries per second.

In its simplest form, the DNS proxy may be implemented as a simple TCP/UDP forwarder, relaying TCP sessions and UDP packets between the DNS client and the destination name server. This can be implemented using off-the-self NAT features in most router/firewall software.

Note Well and Caveats

- Specifying query target using FQDN may be used for both direct instance queries and for queries via proxy.
- If the query target is specified using a FQDN with associated SRV records, it is recommended that all SRV records (i.e. for both TCP and UDP) for a given FQDN resolve to the same set of targets.
- If less than 80% of the anycast locations are responding to queries during Pre-Delegation Testing, the DNS test is failed. It is therefore recommended that all declared locations are configured to answer queries at all times.
- Direct instance queries are performed in addition to queries to the name servers' public addresses intended for use by clients on the Internet.