Finding the Authoritative Registration Data (RDAP) Service
draft-ietf-weirds-bootstrap-01.txt

Abstract

   This document specifies a method to find which Registration Data
   Access Protocol (RDAP) server is authoritative to answer queries for
   a requested scope, such as domain names, IP addresses or Autonomous
   System numbers, using data available in IANA registries.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on August 17, 2014.

Table of Contents

1. Introduction

   Querying and retrieving registration data from registries are defined
   in the Registration Data Access Protocol(RDAP)[I-D.ietf-weirds-rdap-q
   uery][I-D.ietf-weirds-using-http][I-D.ietf-weirds-json-response].
   These documents do not specify where to send the queries. This
   document specifies a method to find which server is authoritative to
   answer queries for the requested scope.

   The proposed mechanism is based on that allocation data for domain
   names and IP addresses are maintained by IANA, are publicly available
   and are in a structured format. The mechanism assumes some data
   structure within these registries and request IANA to modify or
   create these registries for the specific purpose of RDAP use. An
   RDAP client fetches the registries, extract the data and then do a
   match with the query data to find the authoritative registration data
   server and appropriate query base URL.

2. Domain Name RDAP Registry

   The domain names authoritative registration data service is found by
   doing the longest match of the target domain name with the values of
   the Domain column in the IANA Domain Name RDAP registry as defined in
   section Section 9. This is a string search of the longest match
   starting from the end of the target name and the end of each value in
   the Domain column. The value of the "RDAP URL" column is the base
   RDAP url as described in [I-D.ietf-weirds-rdap-query].

   For example, a RDAP query for example.com matches the .com entry in
   the Domain column of the registry. The RDAP server URL for this

address is located in the corresponding "RDAP URL" column for that
entry, which could be http://rdap.example.org/rdap. Therefore the
query URL would be: http://rdap.example.org/rdap/domain/example.com.
This example is not normative.

3. Internet Numbers RDAP Registries

3.1. IPv4 Address Space RDAP Registry

The IPv4 address space authoritative registration data service is
found by doing a longest match of the target address with the values
of the Prefix column in the IANA IPv4 address space RDAP registry as
defined in section Section 9. The longest match is done the same way
as for routing: the addresses are converted in binary form and then
the binary strings are compared. The value of the "RDAP URL" column
is the base RDAP url as described in [I-D.ietf-weirds-rdap-query].

For example, a query for "192.0.2.0/24" matches the "192/8" entry in
the Prefix column of the registry. The RDAP server URL for this
address is located in the corresponding "RDAP URL" column for that
entry, which could be http://rdap.example.org/rdap. Therefore the
query URL would be: http://rdap.example.org/rdap/ip/192.0.2.0/24.
This example is not normative.

3.2. IPv6 Address Space RDAP Registry

The IPv6 address space authoritative registration data service is
found by doing a longest match of the target address with the values
of the Prefix column in the IANA IPv6 address space RDAP registry as
defined in section Section 9. The longest match is done the same way
as for routing: the addresses are converted in binary form and then
the binary strings are compared. The value of the "RDAP URL" column
is the base RDAP url as described in [I-D.ietf-weirds-rdap-query].

For example, a query for "2001:db8::/32" matches the "2001/16" entry
in the Prefix column of the registry. The RDAP server URL for this
address is located in the corresponding "RDAP URL" column for that
entry, which could be http://rdap.example.org/rdap. Therefore the
query URL would be: http://rdap.example.org/rdap/ip/2001:db8::/32.
This example is not normative.

3.3. Autonomous Systems RDAP Registry

The Autonomous Systems (AS) authoritative registration data service
is found by identifying the range in which the target Autonomous
System is, with the values of the Number column in the IANA
Autonomous Systems (AS) Numbers RDAP registry as defined in section

Section 9. The value of the "RDAP URL" column is the base RDAP url
as described in [I-D.ietf-weirds-rdap-query].

For example, a query for AS 65411 matches the "64512-65534" entry in
the Number column of the registry. The RDAP server URL for this
address is located in the corresponding "RDAP URL" column for that
entry, which could be http://rdap.example.org/rdap. Therefore the
query URL would be: http://rdap.example.org/rdap/autnum/65411. This
example is not normative.

4. Entity

Since there is no global namespace for entities, this document does
not describe how to find the authoritative RDAP server for entities.
It is possible however that, if the entity identifier was received
from a previous query, the same RDAP server could be queried for that
entity or the entity identifier itself is a fully referenced URL that
can be queried.

5. Non-existent Entries or RDAP URL Values

The registries may not contain the requested value or the RDAP URL
value may be empty. In these cases, there is no known RDAP server
for that requested value and the client should provide an appropriate
error message to the user.

6. Deployment Considerations

This method relies on the fact that RDAP clients are fetching the
IANA XML registries. Clients SHOULD not fetch every time the XML
files.

If the query data does not match any entry in the already fetched
registry in the client, then the client may implement various
methods, such as the following:

o The client first queries the DNS to see if the respective entry
   has been recently delegated or if it is a mistyped information by
   the user. The DNS query could be to fetch the NS records for a
   domain TLD. If the DNS answer is negative, then there is no need
   to fetch the new version of the XML registry. However, if the DNS
   answer is positive, this means that the currently cached XML
   registry is no more current. The client should fetch the
   registry, parse and then do the normal matching as specified
   above.

o If the client knows the existence of a RDAP aggregator or
   redirector and trust that service, then it could send the query to

the redirector, which would redirect the client if it knows the
authoritative server that client has not found.

o Clients can also rely on HTTP headers to verify if the registry
   has changed since last time it was fetched, without the need to
   fetch the whole registry.

IANA should make sure that the service of those registries is able to
cope with a larger demand and should take appropriate measures such
as caching and load balancing.

This specification makes no assumption on how the authorities of
registration data may work together on sharing their information for
a common service.

7. Limitations

This method does not provide a direct way to find authoritative RDAP
servers:

o for entities

o for queries using search patterns that do not contain a
   terminating string that matches some entries in the registries

8. Security Considerations

By providing a bootstrap method to find RDAP servers, this document
helps making sure that the end-users will get the RDAP data from
authoritative source, instead of from rogue sources. The method
itself has the same security properties as the RDAP protocols
themselves. The transport used to access the registries could be
secured by TLS if IANA supports it.

9. IANA Considerations

IANA is requested to do the following:

o Create a new registry for IPv4 address space with the following
   columns: the first column is the entries taken from the current
   "IPv4 Address Space" registry[ipv4reg] and and the second column
   is the RDAP server URL. The same registrants for these entries
   are entitled to provide the RDAP URL value for their respective
   space, using the same communication channels already established
   between the registrants and IANA.

o Create a new registry for IPv6 address space with the following
   columns: the first column is the entries taken from the current

   IPv6 Address Space registries [ipv6regparent][ipv6reg] and the
   second column is the RDAP server URL. The same registrants for
   these entries are entitled to provide the RDAP URL value for their
   respective space, using the same communication channels already
   established between the registrants and IANA.

   o Create a new registry for Autonomous System Number space with the
      following columns: the first column is the entries taken from the
      current "Autonomous System Number Space" registry[asreg] and the
      second column is the RDAP server URL. The same registrants for
      these entries are entitled to provide the RDAP URL value for their
      respective space, using the same communication channels already
      established between the registrants and IANA.

   o Create a new registry of domain names, essentially TLDs, with the
      following columns: Domain and RDAP URL. The content should be
      initially populated by an extract of the Root zone
      database[domainreg]. The same registrants for these entries are
      entitled to provide the RDAP URL value for their respective space,
      using the same communication channels already established between
      the registrants and IANA.

   o A change happening in any of the source registries should trigger
      a change in the corresponding new registry. For example, a new
      IPv6 address block appearing in the source IPv6 address space
      registry should trigger the same new entry in the corresponding
      RDAP registry.

   o IANA shall update its procedures to include the provisioning of
      these values.

   o It is envisioned that the entries of each of these registries are
      synched from the source assignment registries. There shall be no
      additional records. If there is a need for additional records,
      then the policy for updating the registry is Standards Track RFC.

10. Acknowledgements

   The weirds working group had multiple discussions on this topic,
   including a session during IETF 84. The idea of using IANA
   registries was discovered by the editor during discussions with his
   colleagues as well as by a comment from Andy Newton. All the people
   involved in these discussions are herein acknowledged. Linlin Zhou,
   Jean-Philippe Dionne, John Levine, Kim Davies, Ernie Dainow, Scott
   Hollenbeck, Arturo Servin, Andy Newton have provided input and
   suggestions to this document.

[11](). Non-Normative References

[I-D.ietf-weirds-json-response]
            Newton, A. and S. Hollenbeck, "JSON Responses for the
            Registration Data Access Protocol (RDAP)", draft-ietf-
            weirds-json-response-06 (work in progress), October 2013.

[I-D.ietf-weirds-rdap-query]
            Newton, A. and S. Hollenbeck, "Registration Data Access
            Protocol Query Format", draft-ietf-weirds-rdap-query-10
            (work in progress), February 2014.

[I-D.ietf-weirds-using-http]
            Newton, A., Ellacott, B., and N. Kong, "HTTP usage in the
            Registration Data Access Protocol (RDAP)", draft-ietf-
            weirds-using-http-08 (work in progress), February 2014.

[asreg]   Internet Assigned Numbers Authority(IANA), , "Autonomous
            System (AS) Numbers", <http://www.iana.org/assignments/
            as-numbers/as-numbers.xml>.

[domainreg]
            Internet Assigned Numbers Authority(IANA), , "Root Zone
            Database", <http://www.iana.org/domains/root/db>.

[ipv4reg]   Internet Assigned Numbers Authority(IANA), , "IPv4 Address
            Space", <http://www.iana.org/assignments/
            ipv4-address-space/ipv4-address-space.xml>.

[ipv6reg]   Internet Assigned Numbers Authority(IANA), , "IPv6 Global
            Unicast Address Assignments", <http://www.iana.org/
            assignments/ipv6-unicast-address-assignments/
            ipv6-unicast-address-assignments.xml>.

[ipv6regparent]
            Internet Assigned Numbers Authority(IANA), , "Internet
            Protocol Version 6 Address Space", <http://www.iana.org/
            assignments/ipv6-address-space/ipv6-address-space.xml>.

Author's Address

Marc Blanchet
Viagenie
246 Aberdeen
Quebec, QC G1R 2E1
Canada

Email: Marc.Blanchet@viagenie.ca
URI: http://www.viagenie.ca