Registration Protocols Extensions
Internet-Draft
Intended status: Standards Track
Expires: May 6, 2020

M. Loffredo
M. Martinelli
IIT-CNR/Registro.it

November 3, 2019

Registration Data Access Protocol (RDAP) Reverse search capabilities
draft-ietf-regext-rdap-reverse-search-03

Abstract

The Registration Data Access Protocol (RDAP) does not include query capabilities to find the list of domains related to a set of entities matching a given search pattern. Even if such capabilities, commonly referred as reverse search, respond to some needs not yet readily fulfilled by the current Whois protocol, they have raised concerns from two perspectives: server processing impact and data privacy. Anyway, the impact of the reverse queries on RDAP servers processing is the same as the standard searches and it can be reduced by implementing policies to deal with large result sets, while data privacy risks can be prevented by RDAP access control functionality. In the RDAP context, an entity can be associated to any defined object class. Therefore, a reverse search can be applied to other use cases than the classic domain-entity scenario. This document describes an RDAP search query extension that allows clients to request a reverse search based on the relationship between an object and the associated entities.

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 https://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 May 6, 2020.

Table of Contents

1. Introduction

Reverse Whois is a service provided by many web applications that allow users to find domain names owned by an individual or a company starting from the owner's details, such as name and email. Even if it has been considered useful for some legal purposes (e.g. uncovering trademark infringements, detecting cybercrime cases), its availability as a standardized Whois capability has been objected for two main reasons, which now don't seem to conflict with an RDAP implementation.

The first objection has been caused by the potential risks of privacy violation. However, TLDs community is considering a new generation of Registration Directory Services ([ICANN-RDS1],[ICANN-RDS2],[ICANN-RA]), which provide access to

sensitive data under some permissible purposes and according to adequate policies to enforce the requestor accreditation, authentication, authorization, and terms and conditions of data use. It is well known that such security policies are not implemented in Whois ([RFC3912]), while they are in RDAP ([RFC7481]). Therefore, RDAP permits a reverse search implementation complying with privacy protection principles.

Another objection to the implementation of a reverse search capability has been connected with its impact on server processing. Since RDAP supports search queries, the impact of both standard and reverse searches is equivalent and can be mitigated by servers adopting ad hoc strategies. Furthermore, the reverse search is almost always performed by specifying an entity role (e.g. registrant, technical contact) and this can contribute to restricting the result set.

Reverse searches, such as finding the list of domain names associated with contacts or nameservers may be useful to registrars as well. Usually, registries adopt out-of-band solutions to provide results to registrars asking for reverse searches on their domains. Possible reasons for such requests are:

- the loss of synchronization between the registrar database and the registry database;

- the need for such data to perform massive EPP ([RFC5730]) updates (e.g. changing the contacts of a set of domains, etc.).

Currently, RDAP does not provide any way for a client to search for the collection of domains associated with an entity ([RFC7482]). A query (lookup or search) on domains can return the array of entities related to a domain with different roles (registrant, registrar, administrative, technical, reseller, etc.), but the reverse operation is not allowed. Only reverse searches to find the collection of domains related to a nameserver (ldhName or ip) can be requested. Since an entity can be in relationship with any RDAP object ([RFC7483]), the availability of a reverse search can be common to all resource type path segments defined for search.

The protocol described in this specification aims to extend the RDAP query capabilities to enable the reverse search based on the relationship between any object and the associated entities. The extension is implemented by adding new path segments (i.e. search paths) and using a RESTful web service ([REST]). The service is implemented using the Hypertext Transfer Protocol (HTTP) ([RFC7230]) and the conventions described in RFC 7480 ([RFC7480]).

1.1. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. RDAP Path Segment Specification

The new search paths are OPTIONAL extensions of those defined in RFC 7482 ([RFC7482]). A generic reverse search path is described by the syntax:

{resource-type}/reverse/{role}?{property}=<search pattern>

The path segments are defined as in the following:

- resource-type: it MUST be one of resource type path segments defined in Section 3.2 of RFC 7482 ([RFC7482]): "domains", "nameservers" or "entities";

- role: it MUST be one of the roles described in Section 10.2.4 of RFC 7483 ([RFC7483]). For role independent reverse searches, the value "entity" MUST be used;

- property: it identifies the entity property to be used in matching the search pattern. A pre-defined list of properties includes: fn, handle, email, city, country, cc. The mapping between such properties and the RDAP fields is shown in Table 1. Servers MAY implement additional properties to those defined in this document.

Partial string matching is allowed as defined in section 4.1 of RFC 7482 ([RFC7482]).

Reverse search property	RDAP property	RFC 7483	RFC 6350	RFC 8605
handle	handle	5.1.		
fn	vcard fn		6.2.1	
email	vcard email		6.4.2	
city	locality in vcard adr		6.3.1	
country	country name in vcard adr		6.3.1	
cc	country code in vcard adr			3.1

Table 1: Mapping between the reverse search properties and the RDAP fields

```
https://example.com/rdap/domains/reverse/technical?handle=CID-40*

https://example.com/rdap/domains/reverse/registrant?fn=Bobby*

https://example.com/rdap/domains/reverse/registrant?cc=US

https://example.com/rdap/entites/reverse/registrar?handle=RegistrarX
```

Figure 1: Examples of reverse search queries

The "country" property can be used as an alternative to "cc" when RDAP servers don't include the vCard "cc" parameter ([RFC8605]) in their response.

3. Implementation Considerations

The implementation of the proposed extension is technically feasible. Both handle and fn are used as standard path segments to search for entities ([RFC7482]). With regards to the other reverse search properties, namely email, city and country code, the impact of their usage on server processing is evaluated to be the same as other existing query capabilities (e.g. wildcard prefixed search pattern) so the risks to degrade the performance or to generate huge result sets can be mitigated by adopting the same policies (e.g. restricting the search functionality, limiting the rate of search requests according to the user profile, truncating and paging the results, returning partial responses).

4. Implementation Status

NOTE: Please remove this section and the reference to RFC 7942 prior to publication as an RFC.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in RFC 7942 ([RFC7942]). The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to RFC 7942, "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

4.1. IIT-CNR/Registro.it

Responsible Organization: Institute of Informatics and Telematics of National Research Council (IIT-CNR)/Registro.it
Location: https://rdap.pubtest.nic.it/
Description: This implementation includes support for RDAP queries using data from the public test environment of .it ccTLD.
Level of Maturity: This is a "proof of concept" research implementation.
Coverage: This implementation includes all of the features described in this specification.
Contact Information: Mario Loffredo, mario.loffredo@iit.cnr.it

5. Privacy Considerations

The use of the capability described in this document MUST be compliant with the rules about privacy protection each RDAP provider is subject to. Sensitive registration data MUST be protected and accessible for permissible purposes only. Therefore, RDAP servers MUST provide reverse search only to those requestors who are authorized according to a lawful basis. Some potential users of this capability include registrars searching for their own domains and operators in the exercise of an official authority or performing a

specific task in the public interest that is set out in a law. Another scenario consists of permitting reverse searches, which take into account only those entities that have previously given the explicit consent for publishing and processing their personal data.

6. Security Considerations

Security services required to provide controlled access to the operations specified in this document are described in RFC 7481 ([RFC7481]).

The specification of the entity role within the reverse search path allows the RDAP servers to implement different authorization policies on a per-role basis.

7. IANA Considerations

This document has no actions for IANA.

8. Acknowledgements

The authors would like to acknowledge Tom Harrison, Scott Hollenbeck, Francisco Arias, Gustavo Lozano and Eduardo Alvarez for their contribution to this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3912] Daigle, L., "WHOIS Protocol Specification", RFC 3912, DOI 10.17487/RFC3912, September 2004, <https://www.rfc-editor.org/info/rfc3912>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC6350] Perreault, S., "vCard Format Specification", RFC 6350, DOI 10.17487/RFC6350, August 2011, <https://www.rfc-editor.org/info/rfc6350>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/info/rfc7480>.

[RFC7481] Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", RFC 7481, DOI 10.17487/RFC7481, March 2015, <https://www.rfc-editor.org/info/rfc7481>.

[RFC7482] Newton, A. and S. Hollenbeck, "Registration Data Access Protocol (RDAP) Query Format", RFC 7482, DOI 10.17487/RFC7482, March 2015, <https://www.rfc-editor.org/info/rfc7482>.

[RFC7483] Newton, A. and S. Hollenbeck, "JSON Responses for the Registration Data Access Protocol (RDAP)", RFC 7483, DOI 10.17487/RFC7483, March 2015, <https://www.rfc-editor.org/info/rfc7483>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

[RFC8605] Hollenbeck, S. and R. Carney, "vCard Format Extensions: ICANN Extensions for the Registration Data Access Protocol (RDAP)", RFC 8605, DOI 10.17487/RFC8605, May 2019, <https://www.rfc-editor.org/info/rfc8605>.

9.2. Informative References

[ICANN-RA] Internet Corporation For Assigned Names and Numbers, "Registry Agreement", July 2017, <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf>.

[ICANN-RDS1] Internet Corporation For Assigned Names and Numbers, "Final Report from the Expert Working Group on gTLD Directory Services: A Next-Generation Registration Directory Service (RDS)", June 2014, <https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf>.

[ICANN-RDS2] Internet Corporation For Assigned Names and Numbers, "Final Issue Report on a Next-Generation gTLD RDS to Replace WHOIS", October 2015, <http://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf>.

[REST] Fielding, R., "Architectural Styles and the Design of Network-based Software Architectures", 2000, <http://www.restapitutorial.com/media/RESTful_Best_Practices-v1_1.pdf>.

Appendix A. Change Log

00: Initial working group version ported from draft-loffredo-regext-rdap-reverse-search-04
01: Updated "Privacy Considerations" section.
02: Revised the text.
03: Refactored the query model.

Authors' Addresses

Mario Loffredo
IIT-CNR/Registro.it
Via Moruzzi,1
Pisa 56124
IT

Email: mario.loffredo@iit.cnr.it
URI: http://www.iit.cnr.it

Maurizio Martinelli
IIT-CNR/Registro.it
Via Moruzzi,1
Pisa 56124
IT

Email: maurizio.martinelli@iit.cnr.it
URI: http://www.iit.cnr.it