Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 15, 2020

P. Sood
Google
P. Hoffman
ICANN

May 14, 2020

DNS Resolver Information Self-publication
draft-pp-add-resinfo-01

Abstract

This document describes methods for DNS resolvers to self-publish information about themselves. The information is returned as a JSON object. The names in this object are defined in an IANA registry that allows for light-weight registration. Applications and operating systems can use the methods defined here to get the information from resolvers in order to make choices about how to send future queries to those resolvers.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Historically, DNS stub resolvers typically communicated with the recursive resolvers in their configuration without needing to know anything about the features of the recursive resolvers. More recently, recursive resolvers have different features that may cause stub resolvers to make choices about which configured resolver from its configuration to use, and also how to communicate with the recursive resolver (such as over different transports). Thus stub resolvers need a way to get information from recursive resolvers about features that might affect the communication.

This document specifies a method for stub resolvers to ask recursive resolvers for such information. In short, a new RRtype is defined for stub resolvers to query using the DNS to a special-use domain name.

The response from this method is a JSON object. The JSON object MUST use the I-JSON message format defined in [RFC7493]. Note that [RFC7493] was based on RFC 7159, but RFC 7159 was replaced by [RFC8259]. Requiring the use of I-JSON instead of more general JSON format greatly increases the likelihood of interoperability.

The information that a resolver might want to give to a recursive resolver is not defined in this document; instead other documents

will follow that will specify that information and the format that it comes in.

In nearly every common scenario today, a DNS stub resolver gets the IP addresses of the recursive resolvers that it will use in an insecure fashion, such as from DHCP. Because these addresses were obtained insecurely, the protocol specified here does not try to use authenticated communication. If, in the future, more stub resolvers get the addresses of their recursive resolvers in a secure fashion, this protocol can be enhanced to include authenticated ways of getting information from the resolver.

1.1. Definitions

In the rest of this document, the term "resolver" without qualification means "recursive resolver" as defined in [RFC8499]. Also, the term "stub" is used to mean "stub resolver".

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Retrieving Resolver Information by DNS

A stub that wants to use the DNS to get information about a resolver can use the DNS query defined here. The query a stub resolver uses is resolver-info.arpa/IN/RESINFO. The RRtype "RESINFO" is defined in this document, and the IANA assignment is given in Section 4.1. The contents of the Rdata in the response to this query is defined in Section 3. If the resolver understands the RESINFO RRtype, the RRset in the Answer section MUST have exactly one record.

The name resolver-info.arpa is defined in this document, and the IANA assignment is given in Section 4.3. As described in Section 4.3, the zone resolver-info.arpa is not actually delegated and never will be. The resolver that receives this query acts as if it is delegated, and responds with its own RESINFO data in the Answer section.

A resolver that receives a query with the RRtype of RESINFO with a QNAME of resolver-info.arpa acts as if it is delegated, and responds with its own RESINFO data in the Answer section. The resolver can generate this reply with special code to capture queries for these types of addresses; if the resolver can be configured to also be authoritative for some zones, it can use that configuration to actually be authoritative for the addresses on which it responds.

Any query for the RESINFO RRtype that does not have a QNAME of resolver-info.arpa/IN is meaningless and MUST result in a NODATA or NXDOMAIN response. Resolvers would not need any special code to meet this requirement; they only need code to handle the RESINFO RRtype that is in resolver-info.arpa/IN.

3. Contents of the Returned I-JSON Object

The JSON object returned by a DNS query or an HTTPS query MAY contain any name/value pairs.

All names in the returned object MUST either be defined in the IANA registry or, if for local use only, begin with the substring "temp-". The IANA registry (Section 4.2) will never register names that begin with "temp-".

All names MUST consist only of lower-case ASCII characters, digits, and hyphens (that is, Unicode characters U+0061 through 007A, U+0030 through U+0039, and U+002D), and MUST be 63 characters or shorter. As defined in Section 4.2, the IANA registry will not register names that begin with "temp-", so these names can be used freely by any implementer.

Note that the message returned by the resolver MUST be in I-JSON format. I-JSON requires that the message MUST be encoded in UTF8.

3.1. Example

The I-JSON object that a resolver returns might look like the following:

```
{
   "temp-field2": 42
}
```

As specified in [RFC7493], the I-JSON object is encoded as UTF8. [RFC7493] explicitly allows the returned objects to be in any order.

4. IANA Considerations

4.1. RESINFO RRtype

This document defines a new DNS RR type, RESINFO, whose value TBD will be allocated by IANA from the "Resource Record (RR) TYPEs" sub-registry of the "Domain Name System (DNS) Parameters" registry:

Type: RESINFO

Value: TBD

Meaning: Information self-published by a resolver as an I-JSON (RFC 7493) object

Reference: This document

4.2. Registry for DNS Resolver Information

IANA will create a new registry titled "DNS Resolver Information" that will contain definitions of the names that can be used with the protocols defined in this document. The registration procedure is by Expert Review and Specification Required, as defined in [RFC8126].

The specification that is required for registration can be either an Internet-Draft or an RFC. The reviewer for this registry is instructed to generally be liberal in what they accept into the registry: as long as the specification that comes with the registration request is reasonably understandable, the registration should be accepted.

The registry has the following fields for each element:

Name: The name to be used in the JSON object. This name MUST NOT begin with "temp-". This name MUST conform to the definition of "string" in I-JSON [RFC7493] message format.

Value type: The type of data to be used in the JSON object.

Specification: The name of the specification for the registered element.

4.3. resolver-info.arpa Special-Use Domain Name

IANA will record the domain name "resolver-info.arpa" in the "Special-Use Domain Names" registry [SUDN]. IANA MUST NOT delegate resolver-info.arpa in the .arpa zone.

5. Security Considerations

Unless a DNS request for resolver-info.arpa/IN/RESINFO as described in Section 2 is sent over DNS-over-TLS (DoT) [RFC7858] or DNS-over-HTTPS (DoH) [RFC8484], the response is susceptible to forgery. Given that one of the first expected uses for the protocol in this document is to find out whether DoT or DoH is available for the resolver, it is thus expected that most if not all such DNS requests will be sent without any chance of authentication. Stubs and resolvers SHOULD use

normal DNS methods for avoiding forgery such as query ID randomization and source port randomization.

6. References

6.1. 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>.

[RFC7493] Bray, T., Ed., "The I-JSON Message Format", RFC 7493, DOI 10.17487/RFC7493, March 2015, <https://www.rfc-editor.org/info/rfc7493>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[SUDN] "Special-Use Domain Names", n.d., <https://www.iana.org/assignments/special-use-domain-names/>.

6.2. Informative References

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

Appendix A. Ideas From Earlier Work that was Abandoned

This document is based on work done earlier in the DNSOP working group, and personal drafts before that.

In that earlier work, "<reverse-ip>.{in-addr,ip6}.arpa" was proposed as the domain name to allow for the possibility of DNSSEC-signed responses. However, it was pointed out that people often do not control their reverse IP names and thus their ISP (or their ISP's ISP) could spoof responses and make them look legitimate by signing with DNSSEC.

In an earlier version of this draft, a second way to get the resolver information was specified: using a query to a well-known URI over HTTPS, possibly with authentication. Many participants in the ADD Working Group in early 2020 disagreed with specifying this transport because the IP address being used was most likely obtained by the stub resolver in an insecure fashion, so using an authenticated method could lead to inappropriate assumptions about the security of the answer.

Acknowledgments

The idea of various types of servers publishing information about themselves has been around for decades. However this idea has not been used in the DNS. This document aims to fix this omission.

Roy Arends contributed many ideas to an earlier version of this draft before it was moved to the ADD working group.

Authors' Addresses

Puneet Sood
Google

Email: puneets@google.com

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org