ADD WG
Internet-Draft
Intended status: Standards Track
Expires: October 7, 2021

T. Reddy
McAfee
M. Boucadair
Orange

April 5, 2021

DNS Resolver Information
draft-reddy-add-resolver-info-02

Abstract

This document specifies a method for DNS resolvers to publish information about themselves. Clients can use the resolver information to identify the capabilities of DNS resolvers.

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 October 7, 2021.

Table of Contents

1. Introduction

Historically, DNS stub resolvers communicated with recursive resolvers without needing to know anything about the features supported by these recursive resolvers. As more and more recursive resolvers expose different features that may impact the delivered DNS service, means to help stub resolvers to identify the capabilities of the resolver are valuable. Typically, stub resolvers can discover and authenticate encrypted DNS servers provided by a local network, for example, using the techniques specified in [I-D.ietf-add-dnr] and [I-D.ietf-add-ddr]. However, these stub resolvers need a means to retrieve information from the discovered recursive resolvers about their capabilities.

This document fills that void by specifying a method for stub resolvers to retrieve such information. To that aim, a new RRtype is defined for stub resolvers to query the recursive resolvers. The information that a resolver might want to give is defined in Section 5.

Retrieved information can be used to feed the server selection procedure.

2. Terminology

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.

This document makes use of the terms defined in [RFC8499].

'Encrypted DNS' refers to a DNS protocol that provides an encrypted channel between a DNS client and server (e.g., DoT, DoH, or DoQ).

3. Retrieving Resolver Information

A stub resolver that wants to retrieve the resolver information may use the RRtype "RESINFO" defined in this document (see Section 7.1).

The content of the RDATA in a response to RRtype query is defined in Section 5. If the resolver understands the RESINFO RRtype, the RRset in the Answer section MUST have exactly one record.

The client can retrieve the resolver information using the RESINFO RRtype and QNAME of the domain name that is used to authenticate the DNS server (referred to as ADN in [I-D.ietf-add-dnr]).

If the special use domain name "resolver.arpa" defined in [I-D.ietf-add-ddr] is used to discover the Encrypted DNS server, the client can first retrieve a CNAME that aliases `_dns.resolver.arpa` to `_dns.$HOSTNAME` and then retrieve the resolver information using the RESINFO RRtype and QNAME of the `$HOSTNAME`.

4. Format of the Resolver Information

The resolver information is returned as a JSON object. Precisely, the JSON object MUST use the I-JSON message format [RFC7493].

> Note that [RFC7493] was based on [RFC7159], but [RFC7159] was replaced by [RFC8259]. Requiring the use of I-JSON instead of more general JSON format greatly increases the likelihood of interoperability.

The JSON object returned by a DNS query may contain any name/value pairs. 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). These names MUST be 63 characters or shorter.

All names in the returned object MUST either be defined in the IANA registry Section 7.2 or begin with the substring "temp-" for names defined for local use only.

5. Resolver Information

The resolver information includes the following attributes:

qnameminimization: If the DNS server supports QNAME minimisation [RFC7816] to improve DNS privacy, the parameter value is set to true. This is a mandatory attribute.

extendeddnserror: If the DNS server supports extended DNS error (EDE) [RFC8914] to return additional information about the cause of DNS errors, the parameter lists the possible extended DNS error codes that can be returned by the DNS server. This is an optional attribute.

> Note that the extended error code "Blocked" defined in Section 4.16 of [RFC8914] identifies access to domains is blocked due to an policy by the operator of the DNS server, extended error code "Censored" defined in Section 4.17 of [RFC8914] identifies access to domains is blocked based on a requirement from an external entity and the extended error code "Filtered" defined in Section 4.18 of [RFC8914] identifies access to domains is blocked based on the request from the client to blacklist domains.

clientauth: If the DNS server requires client authentication, the parameter value is set to true. For example, when not on the enterprise network (e.g., coffee shop) yet needing to access the enterprise Encrypted DNS server, roaming users can use client authentication to access the Enterprise-provided Encrypted DNS server. This is an optional attribute.

resinfourl: An URL that points to the generic unstructured resolver information (e.g., DoH APIs supported, possible HTTP status codes returned by the DoH server, how to report a problem) for troubleshooting purpose. The server MUST support the content-type 'text/html'. This is a mandatory attribute.

identityurl: An URL that points to a human-friendly description of the resolver identity to display to the end-user. The server MUST support the content-type 'text/plain'. This is a mandatory attribute.

New attributes can be defined as per the procedure defined in Section 7.2.

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

Figure 1 shows an example of resolver information.

```
{
  "qnameminimization": true,
  "extendeddnserror": [
    15,
    16,
    17
  ],
  "clientauth": false,
  "resinfourl": "https://resolver.example.com/guide",
  "identityurl": "https://resolver.example.com/user-friendly-name"
}
```

Figure 1: An Example of Resolver Information

6. Security Considerations

Unless a DNS request to retrieve the resolver information is encrypted (e.g., sent over DNS-over-TLS (DoT) [RFC7858] or DNS-over-HTTPS (DoH)) [RFC8484], the response is susceptible to forgery. The DNS resolver information can be retrieved after the encrypted connection is established to the DNS server. If the client wishes to retrieve the resolver information before the encryption connection is established to the DNS resolver, the client MUST use local DNSSEC validation.

7. IANA Considerations

Note to the RFC Editor: Please update [RFCXXXX] with the RFC number to be assigned to this document.

7.1. RESINFO RRtype

This document requests IANA to register a new value from the "Resource Record (RR) TYPEs" subregistry of the "Domain Name System (DNS) Parameters" registry available at [RRTYPE]:

Type: RESINFO
Value: TBD
Meaning: Resolver Information as an I-JSON
Reference: [RFCXXXX]

7.2. DNS Resolver Information Registration

This document requests IANA to create a new registry entitled "DNS Resolver Information". This registry contains definitions of the names that can be used to provide the resolver information.

The registration procedure is Specification Required (Section 4.6 of [RFC8126]).

The structure of the registry is as follows:

Name: The name to be used in the JSON object. The name MUST conform to the definition of "string" in I-JSON message format. The IANA registry MUST NOT register names that begin with "temp-", so these names can be used freely by any implementer.

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

Description: Provides a description of the attribute

Specification: The reference specification for the registered element.

The initial content of this registry is provided in Table 1.

Name	Value Type	Specification	Specification
qnameminimization	boolean	Indicates whether qnameminimization is enabled or not	[RFCXXXX]
extendeddnserror	number	Lists the set of extended DNS errors	[RFCXXXX]
clientauth	boolean	Indicates whether client authentication is required or not	[RFCXXXX]
resinfourl	string	Provides an unstructured resolver information that is used for troubleshooting	[RFCXXXX]
identityurl	string	Points to a human-friendly description of the resolver identity to display to the end-user	[RFCXXXX]

Table 1: Initial RESINFO Registry

8. Acknowledgments

This specification leverages the work that has been documented in [I-D.pp-add-resinfo].

Thanks to Tommy Jensen, Vittorio Bertola, Vinny Parla, Chris Box, Ben Schwartz, and Shashank Jain for the discussion and comments.

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>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <https://www.rfc-editor.org/info/rfc7159>.

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

[RFC7816] Bortzmeyer, S., "DNS Query Name Minimisation to Improve Privacy", RFC 7816, DOI 10.17487/RFC7816, March 2016, <https://www.rfc-editor.org/info/rfc7816>.

[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>.

[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>.

[RFC8914] Kumari, W., Hunt, E., Arends, R., Hardaker, W., and D. Lawrence, "Extended DNS Errors", RFC 8914, DOI 10.17487/RFC8914, October 2020, <https://www.rfc-editor.org/info/rfc8914>.

9.2. Informative References

[I-D.pp-add-resinfo]
Sood, P. and P. Hoffman, "DNS Resolver Information Self-publication", draft-pp-add-resinfo-02 (work in progress), June 2020.

[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>.

[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>.

[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>.

[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>.

[RRTYPE] IANA, "Resource Record (RR) TYPEs", <http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>.

Authors' Addresses

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: kondtir@gmail.com

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com