ADD WG
Internet-Draft
Intended status: Standards Track
Expires: September 29, 2021

T. Reddy
McAfee
M. Boucadair
Orange

March 28, 2021

DNS Resolver Information
draft-reddy-add-resolver-info-00

Abstract

This document describes methods for DNS resolvers to publish information about themselves. Applications and operating systems can use the resolver information to identify the capabilities of the resolver.

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 September 29, 2021.

Copyright Notice

Table of Contents

1. Introduction

Historically, DNS stub resolvers typically communicated with the recursive resolvers without needing to know anything about the features of the recursive resolvers. More recently, recursive resolvers have different features that may help the stub resolvers identify the capabilities of the resolver. Thus stub resolvers can discover and authenticate encrypted DNS servers provided by a local network, for example using the techniques proposed in [I-D.ietf-add-dnr] and [I-D.ietf-add-ddr]. Thus stub resolvers need a way to get information from the discovered recursive resolvers about its capabilities.

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 the recursive resolvers. The information that a resolver might want to give is defined in Section 5.

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] and [I-D.ietf-dnsop-terminology-ter].

'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 get information about a resolver can use the RRtype "RESINFO" defined in this document, and the IANA assignment is given in Section 7.1. The contents of the RDATA in the response to this query are 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. The JSON object MUST use the I-JSON message format defined in [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 names in this object are defined in an IANA registry. The JSON object returned by a DNS 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 7.2 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. 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.

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., at home or 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: A 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, etc.) for troubleshooting purpose. This is an optional attribute.

identityurl: A URL that points to a human-friendly description of

the resolver identity to display to the end-user.

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

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

6. Security Considerations

Unless a DNS request to retrieve the resolver information is 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

7.1. 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: Resolver Information as an I-JSON

7.2. DNS Resolver Information Registration

IANA will create a new registry titled "DNS Resolver Information" that will contain definitions of the names that can be used to provide the resolver information. The registration procedure is by Specification Required, as defined in [RFC8126]. 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 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.

IANA will add the names "resinfourl", "identityurl", "extendeddnserror" and "qnameminimization" to the DNS Resolver Information registry.

8. Acknowledgments

This specification leverages the work that has been done 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>.

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

[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>.

[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>.

[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>.

9.2. Informative References

[I-D.ietf-dnsop-terminology-ter]
Hoffman, P., "Terminology for DNS Transports and Location", draft-ietf-dnsop-terminology-ter-02 (work in progress), August 2020.

[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.

[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>.

[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>.

[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>.

[RFC8310] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/info/rfc8310>.

[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>.

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