Workgroup: ADD
Internet-Draft: draft-ietf-add-resolver-info-13
Published: 26 April 2024
Intended Status: Standards Track
Expires: 28 October 2024
Authors: T. Reddy M. Boucadair
Nokia Orange

DNS Resolver Information

Abstract

This document specifies a method for DNS resolvers to publish information about themselves. DNS clients can use the resolver information to identify the capabilities of DNS resolvers. How DNS clients use such an information is beyond the scope of this document.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Adaptive DNS Discovery Working Group mailing list (add@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/add/.

Source for this draft and an issue tracker can be found at https://github.com/boucadair/add-resolver-information.

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 28 October 2024.

Table of Contents

1. Introduction

Historically, DNS clients communicated with recursive resolvers without needing to know anything about the features supported by these resolvers. However, more and more recursive resolvers expose different features that may impact delivered DNS services (privacy preservation, filtering, transparent behavior, etc.). DNS clients can discover and authenticate encrypted DNS resolvers provided by a local network, for example, using the Discovery of Network-designated Resolvers (DNR) [RFC9463] and the Discovery of Designated Resolvers (DDR) [RFC9462]. However, these DNS clients can't retrieve information from the discovered recursive resolvers about their capabilities to feed the resolver selection process. Instead of depending on opportunistic approaches, DNS clients need a more reliable mechanism to discover the features that are configured on these resolvers.

This document fills that void by specifying a mechanism that allows communication of DNS resolver information to DNS clients for use in resolver selection decisions. For example, the resolver selection

procedure may use the retrieved resolver information to prioritize privacy-preserving resolvers over those that don't enable QNAME minimization [RFC9156]. Another example is when a DNS client selects a resolver based on its filtering capability. For instance, a DNS client can choose a resolver that filters domains according to a security policy using the Blocked (15) Extended DNS Error (EDE) [RFC8914]. Alternatively, the client may have a policy not to select a resolver that forges responses using the Forged Answer (4) EDE. However, it is out of the scope of this document to define the selection procedure and policies. Once a resolver is selected by a DNS client, and unless explicitly mentioned, this document does not interfere with DNS operations with that resolver.

Specifically, this document defines a new resource record (RR) type for DNS clients to query the recursive resolvers. The initial information that a resolver might want to expose is defined in Section 5. That information is scoped to cover properties that are used to infer privacy and transparency policies of a resolver. Other information can be registered in the future per the guidance in Section 8.2. The information is not intended for end user consumption.

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]. The following additional terms are used:

Encrypted DNS: Refers to a DNS scheme where DNS exchanges are transported over an encrypted channel between a DNS client and server (e.g., DNS over HTTPS (DoH) [RFC8484], DNS over TLS (DoT) [RFC7858], or DNS over QUIC (DoQ) [RFC9250]).

Encrypted DNS resolver: Refers to a DNS resolver that supports any encrypted DNS scheme.

Reputation: "The estimation in which an identifiable actor is held, especially by the community or the Internet public generally" (Section 1 of [RFC7070]).

3. Retrieving Resolver Information

A DNS client that wants to retrieve the resolver information may use the RR type "RESINFO" defined in this document. The content of the RDATA in a response to a query for RESINFO RR QTYPE is defined in

Section 5. If the resolver understands the RESINFO RR type, the RRSet **MUST** have exactly one record. Invalid records **MUST** be silently ignored by DNS clients. RESINFO is a property of the resolver and is not subject to recursive resolution.

A DNS client can retrieve the resolver information using the RESINFO RR type and the QNAME of the domain name that is used to authenticate the DNS resolver (referred to as the Authentication Domain Name (ADN) in DNR [RFC9463]).

If the Special-Use Domain Name "resolver.arpa", defined in [RFC9462], is used to discover an encrypted DNS resolver, the client can retrieve the resolver information using the RESINFO RR type and QNAME of "resolver.arpa". In this case, a client has to contend with the risk that a resolver does not support RESINFO. The resolver might pass the query upstream, and then the client can receive a positive RESINFO response either from a legitimate DNS resolver or an attacker.

The DNS client **MUST** set the Recursion Desired (RD) bit of the query to 0. The DNS client **MUST** discard the response if the AA flag in the response is set to 0, indicating that the DNS resolver is not authoritative for the response.

If a group of resolvers is sharing the same ADN and/or anycast address, then these instances **SHOULD** expose a consistent RESINFO.

4. Format of the Resolver Information

The resolver information record uses the same format as DNS TXT records. The format rules for TXT records are defined in the base DNS specification (Section 3.3.14 of [RFC1035]) and further elaborated in the DNS-based Service Discovery (DNS-SD) specification (Section 6.1 of [RFC6763]). The recommendations to limit the TXT record size are discussed in Section 6.1 of [RFC6763].

Similar to DNS-SD, the RESINFO RR type uses "key/value" pairs to convey the resolver information. Each "key/value" pair is encoded using the format rules defined in Section 6.3 of [RFC6763]. Using standardized "key/value" syntax within the RESINFO RR type makes it easier for future keys to be defined. If a DNS client sees unknown keys in a RESINFO RR type, it **MUST** silently ignore them. The same rules for the keys as those defined in Section 6.4 of [RFC6763] **MUST** be followed for RESINFO.

Resolver information keys **MUST** either be defined in the IANA registry (Section 8.2) or begin with the substring "temp-" for names defined for local use only.

5. Resolver Information Keys/Values

The following resolver information keys are defined:

qnamemin: The presence of this key indicates that the DNS resolver supports QNAME minimisation [RFC9156] to improve DNS privacy. Note that, per the rules for the keys defined in Section 6.4 of [RFC6763], if there is no '=' in a key, then it is a boolean attribute, simply identified as being present, with no value.

The presence of this key indicates that the DNS resolver is configured to minimise the amount of privacy-sensitive data sent to an authoritative name server.

This is an optional attribute.

exterr: If the DNS resolver supports extended DNS errors (EDE) option [RFC8914] to return additional information about the cause of DNS errors, the value of this key lists the possible extended DNS error codes that can be returned by this DNS resolver. A value can be an individual EDE or a range of EDEs. Range values **MUST** be identified by "-". When multiple non-contiguous values are present, these values **MUST** be comma-separated.

Returned EDEs (e.g., Blocked (15), Censored (16), and Filtered (17)) indicate whether the DNS resolver is configured to reveal the reason why a query was filtered/blocked, when such event happens. If the resolver's capabilities are updated to include new similar error codes, the resolver can terminate the TLS session, prompting the client to initiate a new TLS connection and retrieve the resolver information again. This allows the client to become aware of the resolver's updated capabilities. Alternatively, if the client receives an EDE for a DNS request, but that EDE was not listed in the "exterr", the client can query the resolver again to learn about the updated resolver's capabilities to return new error codes. If a mismatch still exists, the client can identify that the resolver information is inaccurate and discard it.

This is an optional attribute.

infourl: An URL that points to the generic unstructured resolver information (e.g., DoH APIs supported, possible HTTP status codes returned by the DoH server, or how to report a problem) for troubleshooting purposes. The server that exposes such information is called "resolver information server".

The resolver information server **MUST** support only the content-type 'text/html' for the resolver information. The DNS client **MUST** reject invalid the URL if the scheme is not "https". Invalid URLs **MUST** be ignored. The URL **MUST** be treated only as diagnostic

information for IT staff. It is not intended for end user consumption as the URL can possibly provide misleading information.

This key can be used by IT staff to retrieve other useful information about the resolver and also the procedure to report problems (e.g., invalid filtering).

This is an optional attribute.

New keys can be defined as per the procedure defined in Section 8.2.

6. An Example

Figure 1 shows an example of a published resolver information record.

```
resolver.example.net. 7200 IN RESINFO qnamemin exterr=15-17
                      infourl=https://resolver.example.com/guide
```

Figure 1: An Example of Resolver Information Record

As mentioned in Section 3, a DNS client that discovers the ADN "resolver.example.net" of its resolver using DNR will issue a query for RESINFO RR QTYPE for that ADN and will learn that the resolver:

- enables QNAME minimisation,
- can return Blocked (15), Censored (16), and Filtered (17) EDEs, and
- that more information can be retrieved from https://resolver.example.com/guide.

7. Security Considerations

DNS clients communicating with discovered DNS resolvers **MUST** use one of the following measures to prevent DNS response forgery attacks:

1. Establish an authenticated secure connection to the DNS resolver.
2. Implement local DNSSEC validation (Section 10 of [RFC8499]) to verify the authenticity of the resolver information.

It is important to note that, of these two measures, only the first one can apply to queries for 'resolver.arpa'.

An encrypted resolver may return incorrect information in RESINFO. If the client cannot validate the attributes received from the resolver,

that will be used for resolver selection or displayed to the end-user, the client should process those attributes only if the encrypted resolver has sufficient reputation according to local policy (e.g., user configuration, administrative configuration, or a built-in list of reputable resolvers). This approach limits the ability of a malicious encrypted resolver to cause harm with false claims.

8. IANA Considerations

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

8.1. RESINFO RR Type

This document requests IANA to update this entry from the "Resource Record (RR) TYPEs" registry of the "Domain Name System (DNS) Parameters" registry group available at [RRTYPE]:

Type: RESINFO
Value: 261
Meaning: Resolver Information as Key/Value Pairs
Reference: RFCXXXX

8.2. DNS Resolver Information Key Registration

This document requests IANA to create a new registry entitled "DNS Resolver Information Keys" under the "Domain Name System (DNS) Parameters" registry group ([IANA-DNS]). This new registry contains definitions of the keys that can be used to provide the resolver information.

The registration procedure is Specification Required (Section 4.6 of [RFC8126]). Designated experts should carefully consider the security implications of allowing a resolver to include new keys in this registry. Additional considerations are provided in Section 8.3.

The structure of the registry is as follows:

Name: The key name. The name **MUST** conform to the definition in Section 4 of this document. The IANA registry **MUST NOT** register names that begin with "temp-", so these names can be used freely by any implementer.

Description: A description of the registered key.

Specification: The reference specification for the registered element.

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

Name	Description	Specification
qnamemin	The presence of the key name indicates that QNAME minimization is enabled	RFCXXXX
exterr	Lists the set of enabled extended DNS errors. It must be an INFO-CODE decimal value in the "Extended DNS Error Codes" registry.	RFCXXXX
infourl	Provides an URL that points to an unstructured resolver information that is used for troubleshooting	RFCXXXX

Table 1: Initial RESINFO Registry

8.3. Guidelines for the Designated Experts

It is suggested that multiple designated experts be appointed for registry change requests.

Criteria that should be applied by the designated experts include determining whether the proposed registration duplicates existing entries and whether the registration description is clear and fits the purpose of this registry.

Registration requests are evaluated within a three-week review period on the advice of one or more designated experts. Within the review period, the designated experts will either approve or deny the registration request, communicating this decision to IANA. Denials should include an explanation and, if applicable, suggestions as to how to make the request successful.

9. References

9.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[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/rfc/rfc2119>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/rfc/rfc6763>.

[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/rfc/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/rfc/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/rfc/rfc8914>.

[RFC9156] Bortzmeyer, S., Dolmans, R., and P. Hoffman, "DNS Query Name Minimisation to Improve Privacy", RFC 9156, DOI 10.17487/RFC9156, November 2021, <https://www.rfc-editor.org/rfc/rfc9156>.

[RFC9462] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", RFC 9462, DOI 10.17487/RFC9462, November 2023, <https://www.rfc-editor.org/rfc/rfc9462>.

[RFC9463] Boucadair, M., Ed., Reddy.K, T., Ed., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", RFC 9463, DOI 10.17487/RFC9463, November 2023, <https://www.rfc-editor.org/rfc/rfc9463>.

9.2. Informative References

[I-D.pp-add-resinfo] Sood, P. and P. E. Hoffman, "DNS Resolver Information Self-publication", Work in Progress, Internet-Draft, draft-pp-add-resinfo-02, 30 June 2020, <https://datatracker.ietf.org/doc/html/draft-pp-add-resinfo-02>.

[IANA-DNS] IANA, "Domain Name System (DNS) Parameters", <http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4>.

[RFC7070] Borenstein, N. and M. Kucherawy, "An Architecture for Reputation Reporting", RFC 7070, DOI 10.17487/RFC7070, November 2013, <https://www.rfc-editor.org/rfc/rfc7070>.

[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/rfc/rfc7858>.

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

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

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

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

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, Tony Finch, Daniel Kahn Gillmor, Eric Rescorla, Shashank Jain, Florian Obser, Richard Baldry, and Martin Thomson for the discussion and comments.

Thanks to Mark Andrews, Joe Abley, Paul Wouters, and Tim Wicinski for the discussion on the RR formatting rules.

Special thanks to Tommy Jensen for the careful and thoughtful Shepherd review.

Thanks to Johan Stenstam and Jim Reid for the dns-dir reviews, Ray Bellis for the RRTYPE allocation review, Arnt Gulbrandsen for the ART review, and Mallory Knodel for the gen-art review.

Thanks to Eric Vyncke for the AD review.

Thanks to Gunter Van de Velde, Erik Kline, Paul Wouters, Orie Steele, Warren Kumari, Roman Danyliw, and Murray Kucherawy for the IESG review.

Authors' Addresses

Tirumaleswar Reddy
Nokia
India

Email: kondtir@gmail.com

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com