Workgroup: Internet Engineering Task Force
Published: 3 June 2021
Intended Status: Informational
Expires: 5 December 2021
Authors: H. Salgado M. Vergara Ereche
NIC Chile ICANN

The "RRSERIAL" EDNS option for the SOA serial of a RR's zone

Abstract

The "RRSERIAL" EDNS option allows a DNS querier to request a DNS authoritative server to add an EDNS option in the answer of such query with the SOA serial number field of the origin zone which contains the answered Resource Record.

This "RRSERIAL" data allows to debug and diagnose problems by helping to recognize the data source of an answer in an atomic single query, by associating the response with a respective zone version.

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 5 December 2021.

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The "RRSERIAL" EDNS option [RFC6891] allows a DNS querier to request to a DNS authoritative server to add an EDNS option in the answer of such query with the SOA serial number field of the zone associated to the answered Resource Record.

This "RRSERIAL" data allows to help debug by recognizing the data source of an answer, associating this answer with a respective zone version.

DNS data is of loose coherent nature, meaning that a record obtained by a response could be out-of-sync with other authoritative sources of the same data. This makes it difficult to debug responses, because you'd need to couple an answer with the same version of the zone used to obtain such data. Even when you could use a separate query to ask for the SOA RR of the zone and therefore know its SOA serial, such separate query is performed in a different time and could arrive from another authoritative source (for example, in the case the server is anycasted as described in Section 4.9 of [RFC4786]), so it's not directly correlated with the original query.

This EDNS option is aimed to be used only on authoritative servers for a zone. It's intended for hop-to-hop communication (not transitive). Resolver and forwarder behavior is undefined.

The RRSERIAL EDNS extension doesn't offer much relevance for zones served by an Authoritative server that don't use the SOA serial versioning as a meaning to its content. There are cases where

nameservers use different backends for its data sources, like relational databases or by using a different off-DNS synchronicity. In such cases this extension has no benefit or utility to use in debugging or analysis of a response.

1.1. Requirements Language

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. The RRSERIAL Option

The OPTION-CODE for the RRSERIAL option is <TBD>.

The OPTION-DATA for the RRSERIAL option is an unsigned 32 bit version number as defined in the SERIAL field of the "SOA RDATA Format" in Section 3.3.13 of [RFC1035].

The OPTION-LENGTH for the RRSERIAL option MUST have a value of 0 for queries, and MUST have a value of 4 for responses.

3. RRSERIAL Processing

3.1. Initiator

The EDNS RRSERIAL option MAY be included on any QUERY, by adding a zero-length EDNS RRSERIAL option to the options field of the OPT record when the query is made.

3.2. Responder

If an EDNS RRSERIAL option is sent to a server that is Authoritative for the zone queried, and the RCODE for the answer is NOERROR, a name server that understands the RRSERIAL option and chooses to honor a particular RRSERIAL request, MUST put in the OPTION-DATA a copy of the serial field from the SOA Resource Record of the zone which contains the original QNAME of the reply (as per Section 4 of [RFC8499]).

In the case of a SERVFAIL RCODE the responder MAY include the RRSERIAL EDNS option if the QNAME still belongs to an authoritative zone of the server, in which case that serial MUST be the one included in the answer.

Otherwise, the answer MUST NOT add an EDNS RRSERIAL option to the response.

Note that a NODATA response code as defined in Section 3 of [RFC8499] MUST also include the RRSERIAL answer as declared before

even when there's no ANSWER data for the QNAME, as the RCODE corresponds to NOERROR.

4. Example usage

```
$ dig @ns.example.com www.example.com AAAA +rrserial +norec +nocmd

; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16429
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; RRSERIAL: 2019073001
;; QUESTION SECTION:
;www.example.com.                    IN      AAAA

;; ANSWER SECTION:
www.example.com.             900     IN      AAAA

;; Query time: 53 msec
;; SERVER: ns.example.com#53(2001:DB8::53)
;; WHEN: Tue Aug 07 16:54:05 -04 2018
;; MSG SIZE  rcvd: 71
```

Figure 1

5. Acknowledgements

The authors thanks all the comments and support made in the DNSOPS mailing list, chats and discussions.

6. IANA Considerations

6.1. DNS EDNS0 Option Code Registration

Request to IANA for a code point registration for "RRSERIAL" option.

7. Security Considerations

The EDNS extension data it's not covered by RRSIG records, so there's no way to verify its authenticity nor integrity using DNSSEC and could theoricatelly be tampered by a person-in-the-middle if the transport is made by unsecure means. Caution should be taken to use the EDNS RRSERIAL data for any means besides troubleshooting and debugging. If there's a need to certify the RRSERIAL trustwortiness,

it will be necessary to use an encrypted and authenticated DNS transport. If there's a need to authenticate data origin for the RRSERIAL value, it should be compared to a separate regular SOA query with DO flag, whose answer shall be DNSSEC signed, with the cautions about Anycast and others as already stated in Introduction.

There's no risk on disclosure of private information, as the SERIAL of the SOA record is already publicly available.

8. 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/info/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/info/rfc2119>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

9. Informative References

[RFC4786] Abley, J. and K. Lindqvist, "Operation of Anycast Services", BCP 126, RFC 4786, DOI 10.17487/RFC4786, December 2006, <https://www.rfc-editor.org/info/rfc4786>.

[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>.

Appendix A. Implementation References

There's a patched NSD server 4.1.23 with support for RRSERIAL with the experimental opcode 65024 maintained in https://github.com/huguei/nsd/tree/rrserial , and installed for live testing in 200.1.122.30 address with configured zones dateserial.example.com. and incserial.example.com.; with MX, TXT and AAAA apex records.

Authors' Addresses

Hugo Salgado
NIC Chile
Miraflores 222, piso 14
CP 8320198 Santiago
Chile

Phone: +56 2 29407700
Email: hsalgado@nic.cl

Mauricio Vergara Ereche
ICANN

Email: mauricio.vergara@icann.org