Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 23 October 2022

H. Salgado
NIC Chile
M. Vergara Ereche
ICANN

21 April 2022

The "ZONEVERSION" EDNS option for the version token of a RR's zone
draft-ietf-dnsop-zoneversion-00

Abstract

The "ZONEVERSION" EDNS option allows a DNS querier to request a DNS authoritative server to add an EDNS option in the answer of such query with a token field representing the version of the zone which contains the answered Resource Record, such as the SOA serial field in zones when this number corresponds to the zone version.

This "ZONEVERSION" 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 23 October 2022.

Copyright Notice

Table of Contents

1. Introduction

The "ZONEVERSION" 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 a token field representing the version of the zone associated to the answered Resource Record, such as the SOA serial field in zones when this number corresponds to the zone version.

This "ZONEVERSION" 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 in zones where the SOA serial field have the meaning of zone version 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 ZONEVERSION EDNS extension can have different meaning depending on the semantics of the zone maintainer and implementation of nameservers. This document defines one possible value, when the zone version corresponds to the serial field of the SOA Resource Record of the zone, a classic behaviour defined in Section 4.3.5 of [RFC1034].

As the writing of this document, we recognize there are cases where nameservers use different backends for its data sources (like relational databases or by using a different off-DNS synchronicity among others) therefore, the SOA version field doesn't offer much relevance as a versioning to its content, and in those cases the ZONEVERSION EDNS extension SHOULD be extended with a different flag and have an opaque value for its data token.

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 ZONEVERSION Option

The variable part of RDATA in the OPT RR Section 6.1.2 of [RFC6891] for ZONEVERSION is defined as follows:

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

* The OPTION-LENGTH for the ZONEVERSION option MUST have a value of 0 for queries, and MUST have the value of length in octects for the next OPTION-DATA for responses.

* The OPTION-DATA for the ZONEVERSION option is composed of the concatenation of an unsigned 1 byte Flag number, an unsigned 2 bytes number with the Length of the next field in bytes, and the final Data value of the ZONEVERSION field as an opaque bit value, with the previous specified length.

[RFC Editor: change <TBD> to the proper code when assigned by IANA.]

3. ZONEVERSION Processing

3.1. Initiator

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

3.2. Responder

If an EDNS ZONEVERSION option is sent to a server that is Authoritative for the zone, then a name server that understands the ZONEVERSION option and chooses to honor a particular ZONEVERSION request, MUST put in the OPTION-DATA a flag, length and value that corresponds to the properly semantic of such flag number, and corresponds to a zone versioning value of the zone that holds the original QNAME of the reply (as per Section 4 of [RFC8499]).

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

4. ZONEVERSION Flag definition for SOA-SERIAL

The first and only ZONEVERSION Flag defined in this document for the ZONEVERSION Option has the Flag value of 0, a Length field of value 4, and its corresponding Data MUST be a copy of the 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 this ZONEVERSION Option MUST have a value of 7 for responses.

The mnemonic of this flag is SOA-SERIAL.

Note that in this case a NXDOMAIN RCODE already includes the complete SOA Resource Record in the AUTHORITY section, so the inclusion of a ZONEVERSION EDNS Option in the answer is superflous and can be omitted. In the case of a SERVFAIL RCODE the responder MAY include the ZONEVERSION EDNS Option if the QNAME still belongs to an authoritative zone of the server, in which case that value MUST be the one included in the answer.

Note that a NODATA response code as defined in Section 3 of [RFC8499] MUST also include the ZONEVERSION answer even when there's no ANSWER data for the QNAME, since the RCODE is NOERROR.

5. Example usage

A zone which utilizes the serial field of the SOA Resource Record as a number of the zone version release, should answer a ZONEVERSION request with an EDNS option code ZONEVERSION, an OPTION-DATA with a Flag byte with value 0, Length value 4 and a copy of the unsigned 32 bit version number of the SERIAL field of its SOA zone Resourse Record, and an OPTION-LENGTH with value 7.

An example of a proper diagnostic tool that implements ZONEVERSION

EDNS extension towards a compliant authoritative DNS server could be:

```
$ dig @ns.example.com www.example.com AAAA +zoneversion +norec +cmd

; (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
; ZONEVERSION: 2019073001 (SOA-SERIAL)
;; 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

6. Acknowledgements

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

7. IANA Considerations

7.1. DNS EDNS0 Option Code Registration

This document defines a new EDNS0 option, entitled "ZONEVERSION" (see Section 2), and assigns a value of <TBD> from the DNS EDNS0 Option Codes (OPT) Option space:

Value	Name	Status	Reference

<TBD>	ZONEVERSION	Standard	[this document]

Table 1

[RFC Editor: change <TBD> to the proper code when assigned by IANA.]

[RFC Editor: change "this document" with the proper RFC number for this document when assigned by IANA.]

7.2. ZONEVERSION Registry

The ZONEVERSION option also defines a 8-bit Flag field, for which IANA is to create and maintain a new registry entitled "DNS EDNS0 ZONEVERSION Flags values" (abbreviation "ZONEVERSION") used by the ZONEVERSION option, inside the "Domain Name System (DNS) Parameters" group. Initial values for the DNS EDNS0 ZONEVERSION Flags values registry are given below; future assignments in the 1-245 values are to be made through Specification Required Review [BCP26]. Assignments consist of a Flag value as an unsigned 8-bit integer recorded in decimal, a Mnemonic name as an uppercase ASCII string with maximum length of 15 characters, and the required document reference.

ZONEVERSION Flag	Mnemonic	Reference
0	SOA-SERIAL	[this document]
1-245	Unassigned	
246-254	Reserved for Local/	[this document]

	Experimental Use	
255	Reserved for future expansion	[this document]

Table 2

[RFC Editor: change "this document" with the proper RFC number for this document when assigned by IANA.]

The change control for this registry should be my means of an Standard action.

7.2.1. Expert Review Directives

Allocation procedures for new code points in the ZONEVERSION Flag registry require Specification Required review, and so it requires Expert Reviews as stated in [BCP26].

The expert should consider the following points:

* Duplication of code point allocations should be avoided.

* A clear code point mnemonic should be provided.

* The referenced document and stated use of the new code point should be appropriate for the intended use of a ZONEVERSION Flag assignment. In particular the reference should state clear instructions for implementers about the syntax and semantic of the data. Also the Length of the Data must have proper limits.

The expert reviewing the request MUST approve or disapprove the request within 10 business days from when he or she received the expert review request.

8. 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 ZONEVERSION data for any means besides troubleshooting and debugging.

If there's a need to certify the ZONEVERSION trustwortiness, it will be necessary to use an encrypted and authenticated DNS transport.

If there's a need to authenticate data origin for the ZONEVERSION value, an answer with the SOA-SERIAL flag as defined above could 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.

With the SOA-SERIAL flag defined above, there's no risk on disclosure of private information, as the SERIAL of the SOA record is already publicly available.

9. Normative References

[BCP26] 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>.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[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>.

10. 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 version 4.3.7 with support for ZONEVERSION with the experimental opcode 65024 maintained in https://github.com/huguei/nsd/tree/rrserial with SOA-SERIAL flag support, 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