DNSOP Working Group
Internet-Draft
Intended status: Standards Track
Expires: 14 December 2025

E. Bergstrm
J. Stenstam
L. Fernandez
The Swedish Internet Foundation

12 June 2025

Announce Existence of Parent CDS/CSYNC Scanner
draft-berra-dnsop-announce-scanner-00

Abstract

In DNS operations, automated scanners are commonly employed by the operator of a parent zone to detect the presence of specific records, such as CDS or CSYNC, in child zones, indicating a desire for delegation updates. However, the presence and periodicity of these scanners are typically implicit and undocumented, leading to inefficiencies and uncertainties.

This document proposes an extension to the semantics of the DSYNC resource record, as defined in [I-D.draft-ietf-dnsop-generalized-notify], allowing parent zones to explicitly signal the presence and scanning interval of such automated scanners. This enhancement aims to improve transparency and coordination between child and parent zones.

TO BE REMOVED: This document is being collaborated on in Github at: https://github.com/johanix/draft-berra-dnsop-announce-scanner (https://github.com/johanix/draft-berra-dnsop-announce-scanner). The most recent working version of the document, open issues, etc, should all be available there. The authors (gratefully) accept pull requests.

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 14 December 2025.

Table of Contents

1. *1. Introduction* 2
2. *2. DSYNC Record Extension for Scanner Signaling* 3
2.1. *2.1 Signaling Scanner Presence* 3
2.2. *2.2 Signaling Absence of a Scanner* 3
3. *3. Operational Considerations* 4
4. *4. Security Considerations* 4
5. *5. IANA Considerations* 4
6. Informative References 4
Appendix A. Change History (to be removed before publication) . 4
Authors' Addresses 4

1. *1. Introduction*

Automated scanners play a vital role in DNS operations by monitoring zones for specific records that signal desired updates to delegation information. For instance, the presence of CDS records in a child zone indicates a request to update DS records in the parent zone. However, the operation of these scanners is often opaque, with no standardized method for parent zones to signal their presence or scanning frequency.

The lack of explicit signaling can lead to inefficiencies, such as unnecessary scanning or delayed updates due to misaligned expectations between child and parent zones. To address this, this document proposes an extension to the semantics of the DSYNC resource record, enabling parent zones to explicitly announce the presence and scanning interval of their automated scanners.

As the DSYNC record becomes standard automated child-side systems looking up the parent DSYNC records are expected. Given that a vast majority of parent zones do not operate scanners providing a simple mechaism to inform the child of this fact will be useful.

2. *2. DSYNC Record Extension for Scanner Signaling*

The DSYNC resource record, as defined in [I-D.draft-ietf-dnsop-generalized-notify], facilitates the discovery of endpoints for generalized NOTIFY messages. This document proposes an extension to the semantics this record to signal scanner presence (or absence) and periodicity.

The DSYNC record has the following format:

{owner} IN DSYNC {RRtype} {Scheme} {Port} {Target}

For scanner signaling, the fields are interpreted as follows:

* owner: The name of the parent zone.

* RRtype: The type of record the scanner is monitoring (e.g., CDS, CSYNC).

* Scheme: Set to NOTIFY (on the wire this is represented as a uint8 = 1).

* Port: Overloaded to represent the scanning interval in minutes.

* Target: Set to “.” , indicating that this record is for scanner signaling purposes.

2.1. *2.1 Signaling Scanner Presence*

To signal the presence of a CDS scanner that checks for CDS records once every 24 hours, a parent zone would publish the following DSYNC record:

parent.example. IN DSYNC CDS NOTIFY 1440 .

The presence of this record informs the child operator that the parent zone operates a scanner for CDS records with a 1440-minute (= 24h) interval.

2.2. *2.2 Signaling Absence of a Scanner*

To explicitly signal the absence of a scanner, the parent zone would set the port field to 0:

parent.example. IN DSYNC CDS NOTIFY 0 .

The precence of this record indicate that the parent zone does not operate a scanner for CDS records.

3. *3. Operational Considerations*

Publishing DSYNC records (typically for both CDS and CSYNC records) requires no coordination between parent and child zones. The parent zone operator should ensure that the DSYNC records accurately reflect their scanner operations (or absence of a scanner). Child zone operators may use this information to adjust their expectations and processes accordingly.

It’ s important to note that overloading the port field for scanner interval signaling deviates from its original purpose. Hence it is important to first verify that the DSYNC Target field is equivalent to "." before interpreting the Port field as a signaling mechanism rather than a port number.

4. *4. Security Considerations*

The proposed semantic extension does not introduce new security vulnerabilities. However, as with any DNS record, authenticity and integrity should be ensured through DNSSEC signing. Child zones operators should validate the DSYNC records using DNSSEC before trusting them.

5. *5. IANA Considerations*

This document does not require any IANA actions.

6. Informative References

[I-D.draft-ietf-dnsop-generalized-notify]
Stenstam, J., Thomassen, P., and J. R. Levine, "Generalized DNS Notifications", Work in Progress, Internet-Draft, draft-ietf-dnsop-generalized-notify-09, 19 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-generalized-notify-09>.

Appendix A. Change History (to be removed before publication)

Initial public draft

Authors’ Addresses

Erik Bergstrm
The Swedish Internet Foundation
Sweden
Email: erik.bergstrom@internetstiftelsen.se

Johan Stenstam
The Swedish Internet Foundation
Sweden
Email: johan.stenstam@internetstiftelsen.se

Leon Fernandez
The Swedish Internet Foundation
Sweden
Email: leon.fernandez@internetstiftelsen.se