

DNSOP Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 6 March 2026

E. Bergstrm  
J. Stenstam  
L. Fernandez  
The Swedish Internet Foundation  
2 September 2025

Announce Existence of Parent CDS/CSYNC Scanner  
draft-berra-dnsop-announce-scanner-01

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 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 6 March 2026.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction	2
2. Requirements Terminology	3
3. DSYNC Record Extension for Scanner Signaling	3
3.1. Signaling Scanner Presence	3
3.2. Signaling Absence of a Scanner	4
3.3. Wildcard and Child-specific Methods	4
4. Operational Considerations	4
5. Security Considerations	5
6. IANA Considerations	5
7. References	5
7.1. Normative References	5
7.2. Informative References	5
Appendix A. Change History (to be removed before publication)	5
Authors' Addresses	5

## 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 mechanism to inform the child of this fact will be useful.

## 2. Requirements Terminology

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].

## 3. 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 a new {scheme} for this record that can be used to signal scanner presence (or absence) and periodicity. This new scheme=3 is defined as "SCANNER".

The DSYNC record has the following format, as defined in [I-D.draft-ietf-dnsop-generalized-notify]:

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

For scanner signaling, the fields are interpreted as follows:

- \* owner: The name of the parent zone. Follows the discovery methods specified in the DSYNC specification.
- \* RRtype: The type of record the scanner is monitoring (e.g., CDS, CSYNC).
- \* Scheme: Set to SCANNER (on the wire this is represented as a uint8 = 3).
- \* Port: Overloaded to represent the scanning interval in minutes.
- \* Target: Not used, RECOMMENDED to set to ".".

### 3.1. Signaling Scanner Presence

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

```
_dsync.parent.example. IN DSYNC CDS SCANNER 1440 .  
_dsync.parent.example. IN DSYNC CSYNC SCANNER 1440 .
```

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

### 3.2. Signaling Absence of a Scanner

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

```
_dsync.parent.example.  IN DSYNC CDS SCANNER 0 .  
_dsync.parent.example.  IN DSYNC CSYNC SCANNER 0 .
```

The presence of these records indicate that the parent zone does not operate a scanner for CDS or CSYNC records.

### 3.3. Wildcard and Child-specific Methods

Parent zones can also use the wildcard and child-specific methods to signal the presence or absence of scanners as described in [I-D.draft-ietf-dnsop-generalized-notify].

For example:

```
*._dsync.parent.example.  IN DSYNC CDS SCANNER 0 .  
*._dsync.parent.example.  IN DSYNC CSYNC SCANNER 0 .
```

or

```
child._dsync.parent.example.  IN DSYNC CDS SCANNER 0 .  
child._dsync.parent.example.  IN DSYNC CSYNC SCANNER 0 .
```

## 4. 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. Using a new {scheme}, "SCANNER", is intended to minimize the implications of this as software implementations SHOULD discard any unsupported schemes.

## 5. Security Considerations

The proposed new DSYNC scheme does not introduce new security vulnerabilities. As in [I-D.draft-ietf-dnsop-generalized-notify] use of DNSSEC is RECOMMENDED but not required. Hence, a child service that looks up DSYNC RRsets in the parent zone may choose to ignore unsigned DSYNC RRsets.

## 6. IANA Considerations

IANA is requested to assign a new "scheme" value to the registry for "DSYNC Location of Synchronization Endpoints" as follows:

Reference (this document)

RRtype	Scheme	Mnemonic	Purpose	Reference
CDS	3	SCANNER	Scanner announcement	(this document)
CSYNC	3	SCANNER	Scanner announcement	(this document)

## 7. References

### 7.1. 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/rfc/rfc2119>>.

### 7.2. 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 Make sure examples use \_dsync label and propose new scheme

## 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