DNSOP Working Group
Internet-Draft
Intended status: Standards Track
Expires: 13 April 2026

E. Bergstr旦m
J. Stenstam
L. Fernandez
The Swedish Internet Foundation

10 October 2025

Announce Existence of Parent CDS/CSYNC Scanner
draft-berra-dnsop-announce-scanner-02

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 [RFC9859], 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 13 April 2026.

Table of Contents

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", "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.

3. DSYNC Record for Scanner Signaling

The DSYNC resource record, as defined in [RFC9859], facilitates the discovery of endpoints for generalized NOTIFY messages. This document proposes a new {scheme} for the DSYNC record that can be used to signal scanner presence (or absence) and periodicity. This new scheme (with a value=TBD) is represented by the mnemonic "SCANNER".

The DSYNC record has the following format, as defined in [RFC9859]:

{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 with a value TBD).

* Port: This field is NOT USED when scheme=SCANNER. For simplicity it SHOULD be set to 0.

* Target: Used to indicate presence or absence of a scanner. The target "." SHOULD be interpreted as the absence of a scanner.

3.1. Signaling Scanner Presence

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

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

The presence of these records informs the child operator that the parent zone operates a scanner for both CDS and CSYNC records and that any additional information about the scanner is published at the domain name "scanner.parent.example."

Note that there is no need to contact the scanner service as such. The target name is only a domain name used for publication of scanner details.

3.2. Signaling Absence of a Scanner

To explicitly signal the absence of a scanner, the parent would set the "target" field to ".".

_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 [RFC9859].

For example, to indicate the existence of a CDS scanner and the absence of a CSYNC scanner:

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

or

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

3.4. Publishing Additional Scanner Details

There are reasons for the parent to be able to publish additional details about the scanner service (if there is one). These details are published as values in an SVCB record located at the chosen target name.

This document defines two new SVCB keys: "bootstrap" and "interval".

3.4.1. SVCB Key "bootstrap"

The "bootstrap" key is used to signal what mechanisms are supported for upgrading an unsigned delegation to a signed delegation. Three mechanisms are currently identified:

* "rfc8078": This is an indication that the scanner supports automatic DNSSEC onboarding as described in RFC8078. This mechanism requires the child to publish the CDS record at the child apex.

* "rfc9615": This is an indication that the scanner supports automatic DNSSEC onboarding as described in RFC9615. This mechanism requires the child to publish the CDS record both at the child apex and for all authoritative nameservers for the child zone also at the special names "_dsboot.{child}._signal.{nameserver}".

* "manual": This is an indication that the parent supports some other (not based on the scanner, like an EPP transaction) mechanism for DS bootstrap.

The value of the "bootstrap" key is a string with one or more of the defined mechanisms, separated by ",". The mechanisms may occur in arbitrary order.

New mechanisms are expected to be defined in the future. In particular, [I-D.draft-johani-dnsop-delegation-mgmt-via-ddns] has a similar bootstrap need.

3.4.2. SVCB Key "interval"

The "interval" key is used to signal the interval between successive runs of the scanner. The value is time, measured in seconds, between the start time of successive runs. I.e. the value is intended to provide a hint about the maximum wait time before a child-side change is detected by the scanner.

The value is only an indication of the expected scanner interval, not a commitment. It is intended only for human consumption.

3.4.3. Complete Example

Example for a parent that does operate a CDS scanner but not a CSYNC scanner:

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

scanner.parent.example.  IN SVCB 0 . (
bootstrap="rfc8078,rfc9615,manual" interval=86400 )
```

3.5. Publishing Additional Notify-Receiver Details

It is important to be aware that it is possible to operate a scanner without supporting generalized notifications (i.e. no notify-receiver). It is also possible to operate a notify-receiver without operating any scanner.

In the case where there is a notify-receiver but not a scanner, the same information about supported DS bootstrap mechanisms needs to be published. The mechanism for this publication is identical to the mechanism for the scanner details. I.e. it is published as a new key value in an SVCB record located at the DSYNC NOTIFY target:

```
_dsync.parent.example.  IN DSYNC CDS NOTIFY 4711 notify-
receiver.parent.example. _dsync.parent.example.  IN DSYNC CSYNC
NOTIFY 4712 notify-receiver.parent.example. notify-
receiver.parent.example.  IN SVCB 0 . (
bootstrap="rfc8078,rfc9615,manual" )
```

Note that the SVCB key "interval" is not applicable to the notify-receiver, as it only runs a lookup in response to receiving a NOTIFY(CDS), not with a fixed interval.

4. Modification To Child-Side DSYNC Lookup

In [RFC9859] the semantics for looking up the DSYNC RRset are described. This document specifies how to publish additional information of use to the child operator. As this additional information is published at a different owner name (the target field of the relevant DSYNC record) possibly three lookups will be needed to gather all information:

1. First query for "child._dsync.parent.example. DSYNC"

2. If the first query didn’t return an answer, then query for "_dsync.parent.example. DSYNC":

3. If either of the first two queries returned an answer AND information about either DS bootstrapping or scanner interval is relevant THEN query for "{target of DSYNC} SVCB"

It is worth pointing out that the third query is only needed when figuring out how to do DS bootstrap OR provide feedback on the scanner interval.

5. 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 SCANNER" and SVCB records accurately reflect their scanner operations (or absence of a scanner). If a Notify-Receiver exists then the corresponding "DSYNC NOTIFY" and SVCB records correctly describe the operations of the Notify-Receiver. Child zone operators may use this information to adjust their expectations and processes accordingly.

6. Security Considerations

The proposed new "SCANNER" DSYNC scheme does not introduce new security vulnerabilities. As in [RFC9859] 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.

7. 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	[TBD]	SCANNER	Scanner announcement	(this document)
CSYNC	[TBD]	SCANNER	Scanner announcement	(this document)

IANA is also requested to allocate two new entries in the "Service Parameter Keys (SvcParamKeys)" registry.

Number	Name	Meaning	Format Reference	Change Controller	Reference
[TBD]	bootstrap	DS bootstrap mechanisms	(this document)	IETF	(this document)
[TBD]	interval	CDS/CSYNC scanner data	(this document)	IETF	(this document)

8. References

8.1. 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>.

[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>.

[RFC9859] Stenstam, J., Thomassen, P., and J. Levine, "Generalized DNS Notifications", RFC 9859, DOI 10.17487/RFC9859, September 2025, <https://www.rfc-editor.org/rfc/rfc9859>.

8.2. Informative References

[I-D.draft-johani-dnsop-delegation-mgmt-via-ddns] Stenstam, J., Bergstr旦m, E., and L. Fernandez, "Automating DNS Delegation Management via DDNS", Work in Progress, Internet-Draft, draft-johani-dnsop-delegation-mgmt-via-ddns-05, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-johani-dnsop-delegation-mgmt-via-ddns-05>.

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

* draft-berra-dnsop-announce-scanner-02

  Introduce publication of additional data using SVCB at DSYNC target name. Expand scope by adding support for publication of DS bootstrap support in using new SVCB key. Move scanner interval signaling from DSYNC port field to new SVCB key.

* draft-berra-dnsop-announce-scanner-01

  Make sure examples use _dsync label and propose new DSYNC scheme

* draft-berra-dnsop-announce-scanner-00

  Initial public draft

Authors' Addresses

Erik Bergstr旦m
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