Domain Name System Operations
Internet-Draft
Updates: RFC8806 (if approved)
Intended status: Standards Track
Expires: 3 December 2026

W. Hardaker
W. Kumari
Google, Inc.
J. Reid
RTFM llp
G. Huston
APNIC

1 June 2026

An IANA root zone publication source list format
draft-hardaker-dnsop-root-zone-publication-points-02

Abstract

This document describes a machine readable format to be used by IANA to publish a list of sources where the contents of the IANA DNS Root Zone may be fetched from.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-hardaker-dnsop-iana-root-zone-publication-points/.

Discussion of this document takes place on the Domain Name System Operations Working Group mailing list (mailto:dnsop@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/dnsop/. Subscribe at https://www.ietf.org/mailman/listinfo/dnsop/.

Source for this draft and an issue tracker can be found at https://github.com/https://github.com/hardaker/draft-hardaker-dnsop-root-zone-publication-points.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

DNS recursive resolvers implementing functionality such as LocalRoot [draft-wkumari-dnsop-localroot-bcp] need to obtain the contents of the IANA DNS root zone on a regular basis. This document describes a machine readable format that can be used by IANA to publish a list of sources that can be used for obtaining the contents of the IANA DNS Root Zone.

2. IANA maintained list of root zone publication points

The list of IANA root zone data publication points, available at TBD-URL, may be used to discover where the IANA root zone data can be fetched from.

It is expected that this will be used as described in [draft-wkumari-dnsop-localroot-bcp], and may be used by the resolver software directly, or by the operating system a resolver is deployed on, or by a network operator when configuring a resolver.

The contents of the IANA DNS root publication points file MUST be verifiable as to its integrity as having come from IANA and MUST be verifiable as being complete.

2.1. Root zone publication points

NOTE: this is but an example format that is expected to spur discussions within IETF working groups like DNSOP. Whether this is a list in a simple line-delimited format like below or signed JSON or signed PGP or ... is subject to debate.

The IANA root zone data publication points file is structured into two distinct segments, divided by a line consisting of four dashes followed by a newline ("----\n"). The first segment contains a list of URLs, one per line. The second segment provides a signature or cryptographic checksum.

While this specific format was originally designed for IANA’s maintained list of root zone publication points, it may also be used by other publication point aggregation lists.

The list may include URLs using any protocol capable of transferring DNS zone data, including HTTP or HTTPS [RFC9110] (DNS zone file presentation format over HTTP or HTTPS), AXFR [draft-hardaker-dnsop-dns-xfr-scheme], XoT [draft-hardaker-dnsop-dns-xfr-scheme], "XoH" (DNS AXFR over HTTP) [draft-hardaker-dnsop-dns-xfr-scheme], etc. URLs using http or https schemes are for transferring zone file contents in presentation format, not for indicating an AXFR transfer over DNS over HTTPS. URLs for performing an AXFR over the protocol DNS over HTTPS should use the "xoh" scheme instead.

Each URL MUST occur on its own line. Lines beginning with the "#" character are considered comments and MUST be ignored. Leading and trailing whitespace on each line SHOULD be ignored.

Any URLs that reference an unknown transfer protocol in the LocalRoot implementations SHOULD be discarded. If after filtering the list there are no acceptable list elements left, the resolver MUST revert to using regular DNS queries to the IANA root zone instead of operating as a LocalRoot.

The first line of the cryptographic checksum section will contain a checksum or signature type string specifying what the remaining lines in the checksum or signature section will contain. (Ed note: this section is underspecified. We expect to refine this as we get feedback from the working group.)

A minimal example publication point file, containing a single AXFR publication point with a target of b.root-servers.net:

```
http://www.internic.net/domain/root.zone
https://www.internic.net/domain/root.zone
axfr:lax.xfr.dns.icann.org/.
axfr:iad.xfr.dns.icann.org/.
axfr:b.root-servers.net/.
----
SHA256
500c443200c172d81f9811710530c1c244c0b45e702b53ad5bc3a83234f460b3
```

Future note: this should eventually be a signature from an identity, regardless of format, that can be traced back to IANA being the authoritative publisher and not just a simple checksum.

3. Operational Considerations

Implementations SHOULD optimize retrieval to minimize impacts on the server. Because the list is not expected to change frequently, implementations SHOULD refrain from querying IANA’s source more than once a week.

TBD

4. Security Considerations

It is critical that LocalRoot implementations (or other any code bases) making use of the publication point list format described in this document verify the contents using the encoded checksum to ensure it has not been tampered with.

TBD

5. IANA Considerations

TBD: describe the request for IANA to support a list of root server publication points at TBD-URL.

6. References

6.1. Normative References

[BCP237] Best Current Practice 237, <https://www.rfc-editor.org/info/bcp237>. At the time of writing, this BCP comprises the following:

Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/rfc/rfc4033>.

[RFC8976] Wessels, D., Barber, P., Weinberg, M., Kumari, W., and W. Hardaker, "Message Digest for DNS Zones", RFC 8976, DOI 10.17487/RFC8976, February 2021, <https://www.rfc-editor.org/rfc/rfc8976>.

6.2. Informative References

[draft-hardaker-dnsop-dns-xfr-scheme] "The DNS XFR URI Schemes", n.d., <https://datatracker.ietf.org/doc/draft-hardaker-dnsop-dns-xfr-scheme/>.

[draft-hardaker-dnsop-root-zone-publication-list-guidelines] "Guidelines for IANA DNS Root Zone Publication List Providers", n.d., <https://datatracker.ietf.org/doc/draft-hardaker-dnsop-root-zone-publication-list-guidelines>.

[draft-wkumari-dnsop-localroot-bcp] "Populating resolvers with the root zone", n.d., <https://datatracker.ietf.org/doc/draft-wkumari-dnsop-localroot-bcp/>.

[NOROOTS] "On Eliminating Root Nameservers from the DNS", n.d., <https://www.icir.org/mallman/pubs/All19b/All19b.pdf>.

[RFC5936] Lewis, E. and A. Hoenes, Ed., "DNS Zone Transfer Protocol (AXFR)", RFC 5936, DOI 10.17487/RFC5936, June 2010, <https://www.rfc-editor.org/rfc/rfc5936>.

[RFC7766] Dickinson, J., Dickinson, S., Bellis, R., Mankin, A., and D. Wessels, "DNS Transport over TCP - Implementation Requirements", RFC 7766, DOI 10.17487/RFC7766, March 2016, <https://www.rfc-editor.org/rfc/rfc7766>.

[RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/rfc/rfc9110>.

Acknowledgments

TBD

Authors' Addresses

Wes Hardaker
Google, Inc.
Email: ietf@hardakers.net

Warren Kumari
Google, Inc.
Email: warren@kumari.net

Jim Reid
RTFM llp
St Andrews House
382 Hillington Road, Glasgow Scotland
G51 4BL
United Kingdom
Email: jim@rfc1035.com

Geoff Huston
APNIC
6 Cordelia St
South Brisbane QLD 4101
Australia
Email: gih@apnic.net