Workgroup: dnsop
Internet-Draft:
draft-bretelle-dnsop-recursive-iprange-
location-00
Published: 29 October 2020
Intended Status: Standards Track
Expires: 2 May 2021
Authors: E. Bretelle
Facebook

Recursive Resolver

Abstract

This document specifies a way for recursive resolvers operators to signal the IP ranges and locations used by their server pools.

Discussion Venues

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

Source for this draft and an issue tracker can be found at https://github.com/chantra/draft-dns-recursive-iprange-location.

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 2 May 2021.

Copyright Notice

Table of Contents

1. Introduction

Big distributed recursive resolver pools tend to be distributed across the world, operating under multiple countries and possibly using IP ranges for which the country is not necessarily perfectly matching the location of the service. This has lead to sub-optimal answers being returned to those server pools. An solution to this problem has been to use EDNS Client Subnet (ECS) [RFC7871], but this require support from both the recursive resolvers and the name servers authorities, comes with its own Security Considerations, and increased resources usage.

DNS server operators are commonly receiving spoofed DNS traffic over UDP, common techniques have been to reply with TC bit set to force legitimate clients to use TCP, if the load is still too high, they may start to drop traffic from selected subnets. While this may protect their resources, it has the possibility of denying the service to legitimate resolvers.

So far, operators have resorted to ad-hoc mechanism, ranging from exchanging list by email, providing IP ranges and location via webpages, or specific DNS queries, like Google Public DNS, or Cloudflare, or OpenDNS. When web pages are available, they are rarely found at consistent locations, neither are they formatted in a uniform way, essentially making name server operators' task rather complicated and brittle.

This document helps providing uniform solutions to let recursive server operators distribute the list of IP ranges under which their servers are operating as well as possibly location up to the postal code granularity by leveraging [RFC8805] format.

2. Conventions and Definitions

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. Publishing Resolver pool IP ranges

An entity willing to share the IP ranges used by their recursive servers would publish a record under the special name _rdns.example.com. The IP ranges can be distributed either using a TXT record or HTTPS resource record [I-D.ietf-dnsop-svcb-https] An entity can share IP information in 2 ways: via an IP Geolocation Feed, or list of IP ranges in a TXT record.

3.1. TXT Resource Record

An entity that wishes to share the IP ranges they are using with their recursive resolvers can distribute it via a TXT record.

The record is expressed as a single line of text found in the RDATA. Multiple TXT resource records for the same owner name may be permitted.

The record is made of a list of space separated IP ranges with optional comma separated Geolocation. The Geolocation field MUST be a 2-letter ISO country code conforming to ISO 3166-1 alpha 2 [ISO.3166.1alpha2]. Parsers SHOULD treat this field case-insensitively.

This example illustrate a record without geolocation:

```
_rdns.example.com. 3600 IN TXT "192.0.2.0/24 198.51.100.0/24 2001:db8::/
```

This example illustrate a record with geolocation information:

```
_rdns.example.com. 3600 IN TXT "192.0.2.0/24,xa 198.51.100.0/24,xb 2001:
```

As the number of IP ranges increases, the size of the DNS response can become a source for amplification attacks. This is being discussed in Section 4.

3.2. HTTPS Resource Record

Another approach is share an IP geolocation feed [RFC8805] via an HTTPS Resource Record [I-D.ietf-dnsop-svcb-https]. This record has the benefit of providing a format which can provide more granularity if the entity sharing it wishes to, and can scale even when the number of IP ranges increases.

```
_rdns.example.com. 3600 IN HTTPS . (
                            uri=https://foo.example.com/geofeed )
```

4. Security Considerations

Unless the record is DNSSEC-signed [RFC4033], the answers returned cannot be trusted. In HTTPS Resource Record is requested, the client can possibly trust the content if the URI is within the same zone cut, and HTTPS can authenticate the domain.

When using the TXT Resource Record, the answer returned can quickly become big and the name server operator should aggressively limit the size of the answer it will return to the client, and Truncate it if needed.

5. IANA Consideration

5.1. Underscored Node Name

This document updates the IANA registry "Underscored and Globally Scoped DNS Node Names" at https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#underscored-globally-scoped-dns-node-names

The following entries have been added to the registry:

RR Type	HTTPS
Node Name	_rdns
Reference	This document

RR Type	TXT
Node Name	_rdns
Reference	This document

5.2. URI DNS Service Parameter

This document adds a parameter to the "Service Binding (SVCB) Parameter" registry. The allocation request is TBD, taken from the to the First Come First Served range.

If present, this parameters indicates the URI template of an IP Geolocation feed. This is a string encoded as UTF-8 characters.

Name: uri

SvcParamKey	TBD	
Meaning	URI to an IP Geolocation feed	
Reference	This document	

6. Acknowledgments

The authors would like to thank the following individuals for their useful input: John Todd.

7. References

7.1. Normative References

[I-D.ietf-dnsop-svcb-https] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-https-01, 13 July 2020, <http://www.ietf.org/internet-drafts/draft-ietf-dnsop-svcb-https-01.txt>.

[ISO.3166.1alpha2] ISO, "ISO 3166-1 decoding table", <http://www.iso.org/iso/home/standards/country_codes/iso-3166-1_decoding_table.htm>.

[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>.

[RFC8805] Kline, E., Duleba, K., Szamonek, Z., Moser, S., and W. Kumari, "A Format for Self-Published IP Geolocation Feeds", RFC 8805, DOI 10.17487/RFC8805, August 2020, <https://www.rfc-editor.org/info/rfc8805>.

7.2. Informative References

[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/info/rfc4033>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <https://www.rfc-editor.org/info/rfc7871>.

[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/info/rfc8174>.

Author's Address

Emmanuel Bretelle
Facebook

Email: chantra@fb.com