Workgroup: Network Working Group
Internet-Draft:
draft-pauly-add-resolver-discovery-00
Published: 20 May 2020
Intended Status: Standards Track
Expires: 21 November 2020
Authors: T. Pauly
Apple Inc.
E. Kinnear
Apple Inc.
C.A. Wood
Cloudflare
P. McManus
Fastly
T. Jensen
Microsoft

Adaptive DNS Resolver Discovery

Abstract

This document defines a method for dynamically discovering resolvers that support encrypted transports, and introduces the concept of a designating a resolver to be used for a subset of client queries based on domain. This method is intended to work both for locally-hosted resolvers and resolvers accessible over the broader Internet.

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 21 November 2020.

Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

1.1. Specification of Requirements

2. Terminology

3. Designated Resolvers

3.1. Designating with Service Binding DNS Records

3.2. Additional Designation with PvD JSON

3.3. Mutual Confirmation with PvD JSON

4. Explicit Discovery of Local Resolvers

5. Discovery of DoH Capabilities for Direct Resolvers

6. Server Deployment Considerations

6.1. Single Content Provider

6.2. Multiple Content Providers

6.3. Avoid Narrow Deployments

7. Security Considerations

8. Privacy Considerations

9. IANA Considerations

9.1. DoH Template PvD Key

9.2. Trusted Names PvD Key

9.3. DoH URI Template DNS Parameter

9.4. Special Use Domain Name "resolver.arpa"

10. Acknowledgments

11. References

11.1. Normative References

11.2. Informative References

Authors' Addresses

1. Introduction

When clients need to resolve names into addresses in order to establish networking connections, they traditionally use by default the DNS resolver that is provisioned by the local network along with their IP address [RFC2132] [RFC8106]. Alternatively, they can use a resolver indicated by a tunneling service such as a VPN.

However, privacy-sensitive clients might prefer to use an encrypted DNS service other than the one locally provisioned in order to prevent interception, profiling, or modification by entities other than the operator of the name service for the name being resolved. Protocols that can improve the transport security of a client when using DNS or creating TLS connections include DNS-over-TLS (DoT) [RFC7858], DNS-over-HTTPS (DoH) [RFC8484], and Encrypted TLS Client Hellos [I-D.ietf-tls-esni].

This document defines a method for dynamically discovering resolvers that support encrypted transports, and introduces the concept of a designating a resolver to be used for a subset of client queries based on domain. This method is intended to work both for locally-hosted resolvers and resolvers accessible over the broader Internet.

1.1. Specification of Requirements

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.

2. Terminology

This document defines the following terms:

Direct Resolver: A DNS resolver using any transport, encrypted or unencrypted, that is provisioned directly by a local router or a VPN.

Designated Resolver: A DNS resolver that is designated as a responsible resolver for a given domain or zone. Designated resolvers use encrypted transports.

Companion DoH Server: A DNS resolver that provides connectivity over HTTPS (DoH) that is designated as equivalent to querying a particular Direct Resolver.

3. Designated Resolvers

An encrypted DNS resolver, such as a DoH or DoT server, can be designated for use in resolving names within one or more zones. This means that clients can learn about an explicit mapping from a given domain or zone to one or more Designated Resolvers, and use that mapping to select the best resolver for a given query.

Designating a resolver MUST rely on mutual agreement between the entity managing a zone (the Domain Owner) and the entity operating the resolver. These entities can be one and the same, or a Domain Owner can choose to designate a third-party resolver to handle its traffic. Proof of this mutual agreement asserts to clients that sending any query to the designated resolver exposes no more information than sending that query to the entity managing the corresponding zone.

As an example with only one entity, a company that runs many sites within "enterprise.example.com" can provide its own DoH resolver, "doh.enterprise.example.com", and designate only that resolver for all names that fall within "enterprise.example.com". This means that no other resolver would be designated for those names, and clients would only resolve names with the same entity that would service TLS connections.

As an example with several entities, the organization that operates sites within "example.org" may work with two different Content Delivery Networks (CDNs) to serve its sites. It might designate names under "example.com" to two different entities, "doh.cdn-a.net" and "doh.cdn-b.net". These are CDNs that have an existing relationship with the organization that runs "example.org", and have agreements with that organization about how data with information on names and users is handled.

There are several methods that can be used to designate a resolver:

* Based on SVCB DNS records issued to another resolver (Section 3.1)

* Based on information from Designated DoH Resolver that is confirmed via SVCB DNS records (Section 3.2)

* Based on mutual agreement through confirmation of domains over HTTPS (Section 3.3)

Note that clients MUST NOT accept designations for effective top-level domains (eTLDs), such as ".com".

3.1. Designating with Service Binding DNS Records

The primary source for discovering Designated DoH Server configurations is from properties stored in a SVCB (or a SVCB-conformant type like HTTPSSVC) DNS Record [I-D.ietf-dnsop-svcb-httpssvc]. This record provides the URI Template of a DoH server that is designated for a specific domain. A specific domain may have more than one such record.

In order to designate a DoH server for a domain, a SVCB record can contain the "dohuri" (Section 9). The value stored in the parameter is a URI, which is the DoH URI template [RFC8484].

The following example shows a record containing a DoH URI, as returned by a query for the HTTPSSVC variant of the SVCB record type on "foo.example.com", where the response indicates a DoH Resolver that is designated for names under "example.com".

```
foo.example.com.  7200  IN HTTPSSVC 1 example.com. (
                        dohuri=https://doh.example.net/dns-query )
```

If this record is DNSSEC-signed [RFC4033], clients can immediately create a mapping that indicates the server (doh.example.net) as a Designated Resolver for the name in the SVCB record (foo.example.com).

If this record is not DNSSEC-signed, clients MUST perform other validation to determine that the zone designation is permitted, as described in Section 3.3.

3.2. Additional Designation with PvD JSON

A provisioning domain (PvD) defines a coherent set of information that can be used to access a network and resolve names. [I-D.ietf-intarea-provisioning-domains] defines a JSON dictionary format that can be fetched over HTTPS at the well-known URI "/.well-known/pvd".

Designated Resolvers that support DoH SHOULD provide a PvD JSON dictionary available at the well-known PvD URI with the path of the DoH server's URI template appended.

For example, the PvD JSON for the DoH server "https://doh.example.net/dns-query" would be available at "https://doh.example.net/.well-known/pvd/dns-query".

Names that are listed in the "dnsZones" key in the JSON dictionary indicate other names that designate the resolver. For each of those domains, clients SHOULD issue an SVCB query to the DoH resolver. If this record confirms the designation and is DNSSEC-signed, clients can create a mapping to designate the resolver. In order to optimize

the validation of these domains, servers MAY use HTTP Server Push to deliver the records prior to the request being made.

The key "dohTemplate" is also defined within the JSON dictionary (Section 9) to point back to the DoH URI Template itself. This is used for confirming the DoH server when the PvD is discovered locally or during mutual confirmation (Section 3.3).

3.3. Mutual Confirmation with PvD JSON

Designated DoH Resolvers that provide the PvD JSON described in Section 3.2 can also provide information to allow validation of zone designations without DNSSEC.

The JSON dictionary MAY contain a key "trustedNames" that is an array of strings containing domains that can be used for mutual confirmation of resolver designation.

For example, the JSON dictionary retrieved at "https://doh.example.net/.well-known/pvd/dns-query" can contain the following contents:

```
{
  "identifier": "doh.example.net.",
  "dohTemplate": "https://doh.example.net/dns-query",
  "dnsZones": ["example.com"],
  "trustedNames": ["example.com"]
}
```

This indicates that "example.com" should be treated as a designated domain, and that it can be validated by checking with the "example.com" server rather than using DNSSEC.

Clients MUST validate the resolver designation by checking a resource hosted by the name indicated in "trustedNames". The client first issues an HTTP GET request by appending "/.well-known/pvd" to the trusted name, using the "https" scheme. In this example, the resulting URI is "https://example.com/.well-known/pvd". In order to trust the designation, this request must return valid JSON with the "dohTemplate" key matching the original DoH resolver. For example, this dictionary could contain the following contents:

```
{
  "identifier": "example.com.",
  "dohTemplate": "https://doh.example.net/dns-query",
}
```

A client MUST NOT trust a designation if the JSON content is not present, does not contain a "dohTemplate" key, or the value in the

"dohTemplate" key does not match. The following result would not be acceptable for the example above:

```
{
  "identifier": "example.com.",
  "dohTemplate": "https://not-the-doh-youre-looking-for.example.net/d
}
```

Note that the domains listed in "trustedNames" may be broader than the zones that designate the resolver. In the following example, names under "foo.example.com" and "bar.example.com" designate the DoH server "https://doh.example.net/dns-query", and use the PvD JSON from "example.com" to validate the designation. However, the client would not designate the DoH server for all names under "example.com".

```
{
  "identifier": "doh.example.net.",
  "dohTemplate": "https://doh.example.net/dns-query",
  "dnsZones": ["foo.example.com", "bar.example.com"],
  "trustedNames": ["example.com"]
}
```

4. Explicit Discovery of Local Resolvers

If the local network provides configuration with an Explicit Provisioning Domain (PvD), as defined by [I-D.ietf-intarea-provisioning-domains], clients can learn about domains for which the local network's resolver is authoritative. The keys for DoH resolvers described in Section 3.2 also allow this local PvD to be used for resolver discovery.

If an RA provided by the router on the network defines an Explicit PvD that has additional information, and this additional information JSON dictionary contains the key "dohTemplate", then the client SHOULD add this DoH server to its list of known DoH configurations. The domains that the DoH server claims authority for are listed in the "dnsZones" key. Clients MUST use one of the methods for validating a designation described in Section 3.1 or Section 3.3.

Local deployments that want to designate a resolver for a private name that is not easily signed with DNSSEC MUST provide an alternate method of validating a designation, particularly the one described in Section 3.3.

5. Discovery of DoH Capabilities for Direct Resolvers

Direct Resolvers can advertise a Companion DoH server that offers equivalent services and is controlled by the same entity. To do this, a DNS server returns an SVCB record for the "resolver.arpa"

domain with "ipv4hint" and/or "ipv6hint" set to a valid IP address and the "dohuri" key set to a valid DoH URI template as with the Designated DoH Server SVCB record. The TLS certificate used with the DoH URI MUST have the IP addresses for each of its DNS endpoints, classic or DoH, within the SubjectAlternativeName field to allow the client to verify ownership.

Once a client is configured to query a Direct Resolver, it SHOULD query the resolver for SVCB records for the "resolver.arpa" domain before making other queries. This will help the client avoid leaking queries that could go over DoH once the Companion DoH Server is discovered. If an SVCB record is returned, its "dohip" field designates an IP address the client can send DoH queries to in lieu of sending classic DNS queries to the Direct Resolver. The "dohuri" field contains the DoH URI similarly to the SVCB record for a Designated DoH Server.

To validate the Companion DoH Server and the resolver that advertised it are related, the client MUST check the SubjectAlternativeName field of the Companion DoH Server's TLS certificate for the original resolver's IP address and the advertised IP address for the Companion DoH server. If both are present, the discovered Companion DoH Server MUST be used whenever the original Direct Resolver would be used. Otherwise, the client SHOULD suppress queries for Companion DoH Servers against this resolver for the TTL of the negative or invalid response and continue to use the original Direct Resolver.

The following example shows a record containing a Companion DoH URI, as returned by a query for the HTTPSSVC variant of the SVCB record type on the "resolver.arpa" domain.

```
resolver.arpa  7200  IN HTTPSSVC 1 doh.example.net (
                     ipv4hint=x.y.z.w
                     dohuri=https://doh.example.net/dns-query )
```

A DNS resolver MAY return more than one SVCB record of this form to advertise multiple Companion DoH Servers that are valid as a replacement for itself. Any or all of these servers may have the same IP address as the DNS resolver itself. In this case, clients will only have one IP address to check for when verifying ownership of the Companion DoH server.

6. Server Deployment Considerations

When servers designate DoH servers for their names, the specific deployment model can impact the effective privacy and performance characteristics.

6.1. Single Content Provider

If a name always resolves to server IP addresses that are hosted by a single content provider, the name ought to designate a single DoH server. This DoH server will be most optimal when it is designated by many or all names that are hosted by the same content provider. This ensures that clients can increase connection reuse to reduce latency in connection setup.

A DoH server that corresponds to the content provider that hosts content has an opportunity to tune the responses provided to a client based on the location inferred by the client IP address.

6.2. Multiple Content Providers

Some hostnames may resolve to server IP addresses that are hosted by multiple content providers. In such scenarios, the deployment may want to be able to control the percentage of traffic that flows to each content provider.

In these scenarios, there can either be:

* multiple designated DoH servers that are advertised via SVCB DNS Records; or,

* a single designated DoH server that can be referenced by one or more SVCB DNS Records, operated by a party that is aware of both content providers and can manage splitting the traffic.

If a server deployment wants to easily control the split of traffic between different content providers, it ought to use the latter model of using a single designated DoH server that can better control which IP addresses are provided to clients. Otherwise, if a client is aware of multiple DoH servers, it might use a single resolver exclusively, which may lead to inconsistent behavior between clients that choose different resolvers.

6.3. Avoid Narrow Deployments

Using designated DoH servers can improve the privacy of name resolution whenever a DoH server is designated by many different names within one or more domains. This limits the amount of information leaked to an attacker observing traffic between a client and a DoH server: the attacker only learns that the client might be resolving one of the many names for which the server is designated.

However, if a deployment designates a given DoH server for only one name, or a very small set of names, then it becomes easier for an attacker to infer that a specific name is being accessed by a client. For this reason, deployments are encouraged to avoid

deploying a DoH server that is only designated by a small number of names. Clients can also choose to only whitelist DoH servers that are associated with many names.

Beyond the benefits to privacy, having a larger number of names designate a given DoH server improves the opportunity for DoH connection reuse, which can improve the performance of name resolutions.

7. Security Considerations

In order to avoid interception and modification of the information sent between clients and Designated Resolvers, all exchanges between clients and servers are performed over encrypted connections, e.g., TLS.

Malicious adversaries may block client connections to a Designated Resolver as a Denial-of-Service (DoS) measure. Clients which cannot connect these resolvers may be forced to, if local policy allows, fall back to unencrypted DNS if this occurs.

8. Privacy Considerations

Clients must be careful in determining to which DoH servers they send queries directly. A malicious resolver that can direct queries to itself can track or profile client activity. In order to avoid the possibility of a spoofed SVCB record designating a malicious DoH server for a name, clients MUST ensure that such records validate using DNSSEC (Section 3.1) or using mutual confirmation (Section 3.3).

Even servers that are validly designated can risk leaking or logging information about client lookups. Such risk can be mitigated by further restricting the list of resolvers that are whitelisted for direct use based on client policy.

An adversary able to see traffic on each path segment of a DoH query (e.g., from client to a Designated Resolver, and the Designated Resolver to an authoritative DNS server) can link queries to specific clients with high probability. Failure to observe traffic on any one of these path segments makes this linkability increasingly difficult. For example, if an adversary can only observe traffic between a client and proxy and egress traffic from a target, then it may be difficult identify a specific client's query among the recursive queries generated by the target.

9. IANA Considerations

9.1. DoH Template PvD Key

This document adds a key to the "Additional Information PvD Keys" registry [I-D.ietf-intarea-provisioning-domains].

JSON key	Description	Type	Example
dohTemplate	DoH URI Template [RFC8484]	String	"https://dnsserver.example.net/dns-query{?dns}"

Table 1

9.2. Trusted Names PvD Key

This document adds a key to the "Additional Information PvD Keys" registry [I-D.ietf-intarea-provisioning-domains].

JSON key	Description	Type	Example
trustedNames	Names of servers that can validate resolver designation.	Array of Strings	["example.com"]

Table 2

9.3. DoH URI Template DNS Parameter

If present, this parameters indicates the URI template of a DoH server that is designated for use with the name being resolved. This is a string encoded as UTF-8 characters.

Name: dohuri

SvcParamKey: TBD

Meaning: URI template for a designated DoH server

Reference: This document.

9.4. Special Use Domain Name "resolver.arpa"

This document calls for the creation of the "resolver.arpa" SUDN. This will allow resolvers to respond to queries directed at themselves rather than a specific domain name. While this document uses "resolver.arpa" to return SVCB records indicating DoH capability, the name is generic enough to allow future reuse for other purposes where the resolver wishes to provide information about itself to the client.

10. Acknowledgments

Thanks to Erik Nygren, Lorenzo Colitti, Mikael Abrahamsson, Ben Schwartz, Ask Hansen, Leif Hedstrom, Tim McCoy, Stuart Cheshire, Miguel Vega, Joey Deng, Ted Lemon, and Elliot Briggs for their feedback and input on this document.

11. References

11.1. Normative References

[I-D.ietf-dnsop-svcb-httpssvc]
Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPSSVC)", Work in Progress, Internet-Draft, draft-ietf-dnsop-svcb-httpssvc-02, 9 March 2020, <http://www.ietf.org/internet-drafts/draft-ietf-dnsop-svcb-httpssvc-02.txt>.

[I-D.ietf-intarea-provisioning-domains]
Pfister, P., Vyncke, E., Pauly, T., Schinazi, D., and W. Shao, "Discovering Provisioning Domain Names and Data", Work in Progress, Internet-Draft, draft-ietf-intarea-provisioning-domains-11, 31 January 2020, <http://www.ietf.org/internet-drafts/draft-ietf-intarea-provisioning-domains-11.txt>.

[I-D.ietf-tls-esni]
Rescorla, E., Oku, K., Sullivan, N., and C. Wood, "Encrypted Server Name Indication for TLS 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-esni-06, 9 March 2020, <http://www.ietf.org/internet-drafts/draft-ietf-tls-esni-06.txt>.

[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>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

11.2. Informative 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/info/rfc2119>.

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, DOI 10.17487/RFC2132, March 1997, <https://www.rfc-editor.org/info/rfc2132>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[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>.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: tpauly@apple.com

Eric Kinnear
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: ekinnear@apple.com

Christopher A. Wood
Cloudflare
101 Townsend St
San Francisco,
United States of America

Email: caw@heapingbits.net

Patrick McManus
Fastly

Email: mcmanus@ducksong.com

Tommy Jensen
Microsoft

Email: tojens@microsoft.com