Workgroup: add
Internet-Draft: draft-schwartz-svcb-dns-00
Published: 4 August 2020
Intended Status: Standards Track
Expires: 5 February 2021
Authors: B. Schwartz
Google LLC

Service Binding Mapping for DNS URIs

Abstract

The SVCB DNS record type expresses a bound collection of endpoint metadata, for use when establishing a connection to a named service. DNS itself can be such a service, when the server is identified by a hostname in a dns: URI. This document provides the SVCB mapping for name-based DNS URIs, allowing DNS servers to indicate support for new transport protocols.

Discussion Venues

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

Discussion of this document takes place on the ADD Working Group mailing list (add@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/add/.

Source for this draft and an issue tracker can be found at https://github.com/bemasc/svcb-dns.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The SVCB record type [SVCB] provides clients with information about how to reach alternative endpoints for a service, which may have improved performance or privacy properties. The service is typically identified by a URI containing a scheme and an authority (a hostname and optionally a port).

The dns: URI scheme [DNSURI] describes a way to represent DNS queries as URIs. This scheme optionally includes an authority, comprised of a host and port number (with a default of 53). DNS URIs often omit the authority, or specify an IP address, but a hostname is allowed.

Use of the SVCB record type with a URI scheme requires a mapping document, indicating how a client for that scheme can interpret the contents of the SVCB SvcParams. This document provides the mapping for DNS URIs that contain a hostname authority, allowing the server to offer alternative endpoints and transports, including encrypted transports like DNS over TLS and DNS over HTTPS.

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. Name form

Names are formed using Port-Prefix Naming ([SVCB] Section 2.3). For example, dns://dns1.example.com:5353 would be converted to the domain _5353._dns.dns1.example.com..

4. Applicable existing SvcParamKeys

4.1. port

This key is used to indicate the target port for connection. If omitted, the client SHALL use the default port for each transport protocol: 853 for DNS over TLS and 443 for DNS over HTTPS.

This key is automatically mandatory if present.

4.2. alpn and no-default-alpn

These keys indicate the set of supported protocols. The default protocol is "dot", indicating support for DNS over TLS [DOT].

If the protocol set contains any HTTP versions (e.g. "h2", "h3"), then the record indicates support for DNS over HTTPS [DOH], and the "dohpath" key MUST be present (Section 5.1). All keys specified for use with the HTTPS record are also permissible, and apply to the resulting HTTP connection.

If the protocol set contains protocols with different default ports, and no port key is specified, then protocols are contacted separately on their default ports. Note that in this configuration, ALPN negotiation does not defend against cross-protocol downgrade attacks.

These keys are automatically mandatory if present.

4.3. Other applicable SvcParamKeys

These SvcParamKeys apply to the "dns" scheme without modification:

- echconfig
- ipv4hint
- ipv6hint

5. New SvcParamKeys

5.1. dohpath

"dohpath" is a single-valued SvcParamKey whose value (both in presentation and wire format) is a relative URI Template [RFC6570], normally starting with "/". If the "alpn" SvcParamKey indicates support for HTTP, clients MAY construct a DNS over HTTPS URI Template by combining the prefix "https://", the authority hostname from the dns:// URI, the port from the "port" key if present, and the "dohpath" value. (The port from the dns:// URI MUST NOT be used.)

Clients SHOULD NOT query for any "HTTPS" RRs when using the constructed URI Template. Instead, the SvcParams and address records associated with this SVCB record SHOULD be used for the HTTPS connection, with the same semantics as an HTTPS RR. However, for consistency, server operators SHOULD publish an equivalent HTTPS RR, especially if clients might learn this URI Template through a different channel.

6. Limitations

DNS URIs convey limited information to the client. For example, they do not indicate whether the query should include the "recursion desired", "DNSSEC OK", or "checking disabled" flags. Clients must know the appropriate values for these flags in their use case. Similarly, nothing in this document indicates the set of names for which the server is willing or able to answer queries.

7. Examples

- A resolver at dns://resolver.example that supports
  - DNS over TLS on resolver.example, port 853 and 8530, with resolver.example as the Authentication Domain Name,

- DNS over HTTPS at https://resolver.example/dns-query{?dns}, and

- an experimental protocol on fooexp.resolver.example:5353:

```
$ORIGIN example.
_dns.resolver 7200 IN SVCB 1 resolver (
  alpn=h2,h3 echconfig=... dohpath=/dns-query{?dns} )
_dns.resolver 7200 IN SVCB 2 resolver (
  port=8530 echconfig=... )
_dns.resolver 7200 IN SVCB 3 fooexp.resolver ( port=5353
  echconfig=... alpn=foo no-default-alpn foo-info=... )
```

* A nameserver at dns://ns.example whose service configuration is published on a different domain:

```
$ORIGIN example.
_dns.ns 7200 IN SVCB 0 _dns.ns.nic
```

8. Security Considerations

8.1. Adversary on the query path

This section considers an adversary who can add or remove responses to the SVCB query.

Clients MUST authenticate the server to its name during secure transport establishment. This name is the hostname present in the DNS URI, and cannot be influenced by the SVCB record contents. Accordingly, this draft does not mandate the use of DNSSEC. This draft also does not specify how clients authenticate the name (e.g. selection of roots of trust), which might vary according to the context.

Although this adversary cannot alter the authentication name of the server, it does have control of the port number and "dohpath" value. As a result, the adversary can direct DNS queries for "dns://$HOSTNAME" to any port on $HOSTNAME, and any path on "https://$HOSTNAME", even if $HOSTNAME is not actually a DNS server. If the DNS client uses shared TLS or HTTP state, the client could be correctly authenticated (e.g. using a TLS client certificate or HTTP cookie).

This behavior creates a number of possible attacks for certain server configurations. For example, if "https://$HOSTNAME/upload" accepts any POST request as a file upload, the adversary could forge a SVCB record containing dohpath=/upload, causing the client to upload every query, resulting in unexpected storage costs.

As a mitigation, a client of this SVCB mapping MUST NOT provide client authentication for DNS queries, except to servers that it specifically knows are not vulnerable to such attacks. Also, if an alternative service endpoint sends an invalid response to a DNS query, the client SHOULD NOT send more queries to that endpoint.

8.2. Adversary on the transport path

This section considers an adversary who can modify network traffic between the client and the SvcDomainName (i.e. the destination server).

A client that attempts a connection using an encrypted DNS transport from a SVCB record SHOULD NOT fall back to unencrypted DNS if connection fails. (This is different from the advice in Section 3 of [SVCB], which assumes the default transport is secured.) Specifications making using of this mapping MAY adjust this fallback behavior to suit their requirements.

9. IANA Considerations

Per [SVCB] IANA would be directed to add the following entry to the SVCB Service Parameters registry.

Number	Name	Meaning	Reference
TBD	dohpath	DNS over HTTPS path template	(This document)

Table 1

Per [Attrleaf], IANA would be directed to add the following entry to the DNS Underscore Global Scoped Entry Registry:

RR TYPE	_NODE NAME	Meaning	Reference
SVCB	_dns	DNS SVCB info	(This document)

Table 2

10. References

10.1. Normative References

[DNSURI] Josefsson, S., "Domain Name System Uniform Resource Identifiers", RFC 4501, DOI 10.17487/RFC4501, May 2006, <https://www.rfc-editor.org/info/rfc4501>.

[DOH] 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>.

[DOT] 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>.

[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>.

[RFC6570] Gregorio, J., Fielding, R., Hadley, M., Nottingham, M., and D. Orchard, "URI Template", RFC 6570, DOI 10.17487/RFC6570, March 2012, <https://www.rfc-editor.org/info/rfc6570>.

[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>.

[SVCB] 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>.

10.2. Informative References

[Attrleaf] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <https://www.rfc-editor.org/info/rfc8552>.

Acknowledgments

TODO acknowledge.

Author's Address

Benjamin Schwartz
Google LLC

Email: bemasc@google.com