Workgroup:	Internet Engineering Task Force
Internet-Draft:	draft-cridland-dns-svcbop-xmpp-00
Published:	12 February 2024
Intended Status:	Standards Track
Expires:	15 August 2024
Author:	D. A. Cridland
	XMPP Standards Foundation

Title

Abstract

XMPP was originally specified to be accessed over a simple TCP binding, however there are now multiple bindings including TCP, TLS, QUIC, Websocket and BOSH. Discovery of connection options has been historically difficult, and although XMPP uses SRV records to facilitate TCP and TLS discovery, web bindings have made this more complex. This memo defines an SVCB mapping for XMPP services, allowing them to indicate all current connection mechanisms.

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 15 August 2024.

Copyright Notice

Table of Contents

1. Introduction

XMPP has historically used SRV records to indicate the hostname and port for a given service domain. This is defined within [RFC6120] only for the basic TCP binding, but [XEP-0368] adds a further SRV label (and an ALPN Protocol ID) for the variants operating directly over TLS (instead of using StartTLS). This requires clients to look up two SRV records before combining the results and connecting. [XEP-0206] provides a web binding using an HTTP "long polling" technique, and [RFC7395] then introduces a WebSocket binding. Additionally, [XEP-0467] defines a QUIC binding, and [XEP-0468] defines a websocket binding for the server-to-server (S2S) protocol.

Many mechanisms for discovering all possible bindings have been proposed. These include [XEP-0156], [RFC7711], and [HOST-META-2]. These have often introduced additional HTTPS requests or multiple DNS queries.

Therefore this memo proposes a mechanism for using SVCB records with XMPP, in line with Section 2.4.3 of Section 2.4.3 of [RFC9460].

1.1. Conventions used in this document

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.

The word "client" is used here in the sense used within SVCB; in [RFC6120] this would correspond to "Initiating Entity". In particular, a "client" may well be an XMPP server.

2. SVCB QNAME Formation

An XMPP service domain is typically referenced only by the domain itself, without any port specified. Therefore it is not expected that a port prefix will be used.

On the other hand, there are typically two pseudo-schemes used. Servers connecting to one another for the purposes of federation will use the SRV label "xmpp-server", whereas clients connecting to their home service will use "xmpp-client". Both labels are therefore defined here.

Of particular note is that XMPP servers often host multiple related domains - for example, on a server where users are within the domain "example.net", group chat services might reside at "conference.example.net"; however nothing in this specification allows a connecting server to assume that records for "_xmpp-server.conference.example.net" are the same as "_xmpp-server.example.net".

3. Applicable Existing SvcParamKeys

3.1. "alpn"

This key indicates the set of supported protocols (Section 7.1 of Section 7.1 of [RFC9460]). There is no default protocol, and so the "no-default-alpn" key does not apply. In the absence of an "alpn" key, the client MUST assume that this record indicates an RFC 6920 TCP (ie, StartTLS) binding.

If the protocol set contains any HTTP versions, then the record indicates support for a web binding, and either (or both) of the "bosh" or "xmpp-ws" key MUST be present.

3.2. "port"

This key indicates the port to connect to. If omitted, the client SHALL use the default port. Note that while "xmpp-server" and "xmpp-client" have default ports, and the web bindings use the HTTP default ports, "xmpps-server" and "xmpps-client" have a default port registered in this document.

This key is "automatically mandatory" for this binding.

4. Other Applicable SvcParamKeys

"mandatory", "ipv4hint", and "ipv6hint" all apply to this specification as-is.

5. New SvcParamKeys

5.1. "bosh"

This key defines an HTTP path for the BOSH [XEP-0206] binding. It MUST NOT appear unless an HTTP protocol appears in the "alpn" key.

5.2. "xmpp-ws"

This key defines an HTTP path for the WebSocket [RFC7395] binding. It MUST NOT appear unless an HTTP protocol appears in the "alpn" key.

6. Use with web bindings

Clients which operate entirely within a web browser - the original targets of the web bindings - cannot use arbitrary DNS lookups. Deployments therefore SHOULD provide HTTPS records, and MAY provide a [XEP-0156] service in addition.

Clients connecting to a web binding use the XMPP service domain as the name for authentication unless SVCB record is DNSSEC signed, as per [RFC9525]. If a service uses a different name, and DNSSEC is unavailable, then [XEP-0156] provides a discovery mechanism that allows the hostname to be securely changed.

7. Usage in implementations

It is assumed that a given implementation will support a range of bindings, and moreover will have an internal preference. For example, it might prefer XEP-0368 over RFC 6120, or might be only capable of using the web bindings.

Therefore, the procedure for connecting is as follows:

1. First, perform an SVCB query.
2. Order the returned records by SvcPriority.
3. If the lowest priority is 0, then follow the AliasMode record, returning to step 1
4. Otherwise, pick a random record from those with the lowest priority. Clients MAY implicitly weight them by their internal preference rather then truly randomly picking, but MUST honour the defined SvcPriority.
5. Discard any "alpn" values that are unsupported by the client. If no "alpn" values remain, discard the record and return to step 4.
6. Proceed to connect by the remaining protocols, in order of the internal preference.

For example, in the case of an XMPP Server wishing to federate to "pubsub.example.net", which does not support WebSockets, and prefers direct TLS over StartTLS, given the following records:

- _xmpp-server.pubsub.example.net. IN SVCB 0 xmpp.example.net. ;; AliasMode
- xmpp.example.net IN SVCB 1 . alpn=http/1.1,h2 port=5280 xmpp-ws=/xmpp-s2s-ws ;; WebSocket binding [RFC7395]>
- xmpp.example.net IN SVCB 2 . alpn=xmpp-server port=5270 ;; Immediate-mode TLS [XEP-0368]
- xmpp.example.net IN SVCB 2 . ;; TCP (StartTLS) binding [RFC6120]

The server will initially fetch the SVCB AliasMode record, and issue a second DNS query for SVCB on "xmpp.example.net".

It will then order the records and select the first, which is a WebSocket binding it does not support. This will be discarded.

Next, it will examine the two records at the next highest priority. These are equal priority, but the server prefers to use the direct TLS binding, and so picks that record first.

8. Differences to existing discovery mechanisms

8.1. SRV

Administrators familiar with SRV will note the following changes:

1. There is no mechanism to specify a "weight" within the SvcPriority. This has never been used heavily within the XMPP landscape.
2. SVCB's AliasMode allows simpler deployment for multiple service domains.

8.2. XEP-0156

1. [XEP-0156] causes the authenticated name to change.
2. [XEP-0156] introduces an HTTP request, which in turn needs to use SVCB queries for efficiency.

9. IANA Considerations

This memo includes no request to IANA, although it definitely should.

10. Security Considerations

Compared the SRV, this specification is not thought to introduce any additional security concerns.

Compared to [XEP-0156], this specification reduces the attack surface, though the authenticated name change is bound to trip everyone up.

11. References

11.1. 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/info/rfc2119>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[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>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/info/rfc9460>.

[RFC9525] Saint-Andre, P. and R. Salz, "Service Identity in TLS", RFC 9525, DOI 10.17487/RFC9525, November 2023, <https://www.rfc-editor.org/info/rfc9525>.

11.2. Informative References

[RFC7711] Miller, M. and P. Saint-Andre, "PKIX over Secure HTTP (POSH)", RFC 7711, DOI 10.17487/RFC7711, November 2015, <https://www.rfc-editor.org/info/rfc7711>.

[RFC7395] Stout, L., Ed., Moffitt, J., and E. Cestari, "An Extensible Messaging and Presence Protocol (XMPP) Subprotocol for WebSocket", RFC 7395, DOI 10.17487/RFC7395, October 2014, <https://www.rfc-editor.org/info/rfc7395>.

[XEP-0156] Hildebrand, J., Saint-Andre, P., and L. Stout, "Discovering Alternative XMPP Connection Methods", 2022, <https://xmpp.org/extensions/xep-0156.html>.

[XEP-0206] Paterson, I., Saint-Andre, P., Stout, L., and W. Tilanus, "XMPP Over BOSH", 2014, <https://xmpp.org/extensions/xep-0206.html>.

[XEP-0368] Burtrum, T., "SRV records for XMPP over TLS", 2019, <https://xmpp.org/extensions/xep-0368.html>.

[XEP-0467] Burtrum, T., "XMPP over QUIC", 2022, <https://xmpp.org/extensions/xep-0467.html>.

[XEP-0468] Burtrum, T., "WebSocket S2S", 2022, <https://xmpp.org/extensions/xep-0468.html>.

[HOST-META-2] Burtrum, T., "Host Meta 2 - One Method To Rule Them All", 2023, <https://xmpp.org/extensions/inbox/host-meta-2.html>.

Acknowledgements

I look forward to ackowledging the help I undoubtedly need.

Contributors

You name here!

Author's Address

Dave Cridland
XMPP Standards Foundation
Email: dave@cridland.net
URI: https://www.xmpp.org/