XEP-0156: Discovering Alternative XMPP Connection Methods

Joe Hildebrand
mailto:jhildebr@cisco.com
xmpp:hildjj@jabber.org

Peter Saint-Andre
mailto:stpeter@stpeter.im
xmpp:stpeter@jabber.org
https://stpeter.im/

Lance Stout
mailto:lance@andyet.com
xmpp:lance@lance.im

2022-02-10
Version 1.4.0

Status	Type	Short Name
Draft	Standards Track	alt-connections

This document defines an XMPP Extension Protocol for discovering alternative methods of connecting to an XMPP server via Web Host Metadata Link format.

Legal

Copyright

Permissions

Warranty

Liability

Conformance

Contents

1 Introduction

Although XMPP Core [1] specifies the use of TCP as the method of connecting to an XMPP server, alternative connection methods exist, including the BOSH (XEP-0124) [2] method (for which XMPP Over BOSH (XEP-0206) [3] is the XMPP profile) and the websocket subprotocol specified in RFC 7395 [4]. For some of these methods, it is necessary to discover further parameters before connecting, such as the HTTP URL of an alternative connection manager. Without ways to auto-discover alternative connection methods, the relevant information would need to be provided manually by a human user (which is cumbersome and error-prone) or hard-coded into XMPP software applications (which is brittle and not interoperable).
This document defines a way to encapsulate information about alternative connection methods for auto-discovery via Link entries in a server's "host-meta" file.

2 HTTP Lookup Method

2.1 Link Format

The HTTP lookup method uses Web Host Metadata RFC 6415 [5] to categorize and list the URIs of alternative connection methods. It is primarily intended for use by clients in environments where the ability to perform DNS queries is restricted, such as in web browsers.
Each alternative connection method is specified in the host-meta (XRD) file using a distinctive link relation RFC 5988 [6]. This specification defines several extension relation types:

- urn:xmpp:alt-connections:websocket
- urn:xmpp:alt-connections:xbosh

2.2 Business Rules

The following business rules apply:

1. host-meta files MUST be fetched only over HTTPS, and MUST only use connection URLs starting with 'https://' or 'wss://'. This provides secure delegation, meaning you SHOULD send SNI matching the host of the URL from the connection URL and validate that the certificate is valid for that host *or* the XMPP domain.

[1] RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <http://tools.ietf.org/html/rfc6120>.
[2] XEP-0124: Bidirectional-streams Over Synchronous HTTP <https://xmpp.org/extensions/xep-0124.html>.
[3] XEP-0206: XMPP Over BOSH <https://xmpp.org/extensions/xep-0206.html>.
[4] RFC 7395: An Extensible Messaging and Presence Protocol (XMPP) Subprotocol for WebSocket <http://tools.ietf.org/html/rfc7395>.
[5] RFC 6415: Web Host Metadata <http://tools.ietf.org/html/rfc6415>.
[6] RFC 5988: Web Linking <http://tools.ietf.org/html/rfc5988>.

2. Services implementing this XEP MUST offer the information in the Extensible Resource Descriptor (XRD) format and SHOULD additionally provide the JRD format (both formats are specified in RFC 6415 [7]).

3. HTTPS queries for host-meta information MUST be used only as a fallback after the methods specified in RFC 6120 have been exhausted.

4. A domain SHOULD NOT present information in host-meta link records that is available via the DNS SRV records defined in RFC 6120.

5. The order of XMPP related link entries in the host-meta file SHOULD NOT be interpreted as significant by the presenting domain or the receiving entity.

2.3 Examples

The following examples show two host-meta link records: the first indicates support for the XMPP Over BOSH connection method defined in XEP-0124 and XEP-0206 and the second indicates support for the XMPP Over WebSocket connection method defined in RFC 7395 [8].

Listing 1: Result for /.well-known/host-meta

```
<?xml version='1.0' encoding='utf-8'?>
<XRD xmlns='http://docs.oasis-open.org/ns/xri/xrd-1.0'>
  ...
  <Link rel="urn:xmpp:alt-connections:xbosh"
        href="https://web.example.com:5280/bosh" />
  <Link rel="urn:xmpp:alt-connections:websocket"
        href="wss://web.example.com:443/ws" />
  ...
</XRD>
```

It is possible to use additionally a JSON-based format for host-meta information. The JSON representation of the host metadata is named JRD and specified in Appendix A of RFC 6415 [9]. The above XRD example would be presented in JRD as:

Listing 2: Result for /.well-known/host-meta.json

```
{
  ...
  "links": [
    ...
    {
      "rel": "urn:xmpp:alt-connections:xbosh",
```

[7] RFC 6415: Web Host Metadata <http://tools.ietf.org/html/rfc6415>.
[8] RFC 7395: An Extensible Messaging and Presence Protocol (XMPP) Subprotocol for WebSocket <http://tools.ietf.org/html/rfc7395>.
[9] RFC 6415: Web Host Metadata <http://tools.ietf.org/html/rfc6415>.

```
      "href": "https://web.example.com:5280/bosh"
    },
    {
      "rel": "urn:xmpp:alt-connections:websocket",
      "href": "wss://web.example.com:443/ws"
    }
  ]
}
```

3 Implementation Notes

To make connection discovery work in web clients (including those hosted on a different domain) the host service SHOULD set appropriate CORS headers for Web Host Metadata files. The exact headers and values are out of scope of this document but may include: *Access-Control-Allow-Origin*, *Access-Control-Allow-Methods* and *Access-Control-Allow-Headers*.
Due care has to be exercised in limiting the scope of *Access-Control-Allow-Origin* response header to Web Host Metadata files only.

```
Access-Control-Allow-Origin: *
```

Access-Control-Allow-Origin header with a value of * allows JavaScript code running on a different domain to read the content of Web Host Metadata files. Special value * ensures that the request will only succeed if it is invoked without user credentials (e.g. cookies, HTTP authentication).

4 Security Considerations

It is possible that advertisement of alternative connection methods can introduce security vulnerabilities, since a connecting entity (usually a client) might deliberately seek to connect using the method with the weakest security mechanisms (e.g., no channel encryption or relatively weak authentication). Care needs to be taken in determining which alternative connection methods are appropriate to advertise or implement in your lookup.
Entities that use these connection methods MUST only fetch host-meta over Transport Layer Security (TLS), and MUST only use 'https' or 'wss' URLs that are protected using TLS.
A previous version of this XEP defined a DNS method to look up this info using a TXT *_xmpp-connect* record, this was insecure and has been removed.

5 IANA Considerations

Because the link relations specified here are extension relation types rather than registered relation types (see Section 4 of RFC 5988), this document requires no interaction with the

Internet Assigned Numbers Authority (IANA) [10].

6 XMPP Registrar Considerations

6.1 Namespaces

The XMPP Registrar [11] shall include 'urn:xmpp:alt-connections' in its registry of protocol namespaces (see <https://xmpp.org/registrar/namespaces.html>).

- urn:xmpp:alt-connections

[10] The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.

[11] The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <https://xmpp.org/registrar/>.