Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 16, 2018

P. Hallam-Baker
Comodo Group Inc.

June 14, 2018

DNS Web Service Discovery
draft-hallambaker-web-service-discovery-00

Abstract

This document describes a standardized approach to discovering Web Service Endpoints from a DNS name. Services are advertised using the DNS SRV and TXT records and the HTTP Well Known Service conventions.

This document is also available online at http://mathmesh.com/Documents/draft-hallambaker- web-service-discovery.html [1] .

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 December 16, 2018.

Table of Contents

1. Introduction

Web services are traditionally identified by means of a URI specifying a Web Service Endpoint (WSE). This is approach is unsatisfactory in many situations:

Specification of the Web Service requires the transport and presentation protocols to be fixed.

The discovery mechanism does not provide support for load balancing or fault tolerance.

The identifiers are unsuited for human interaction.

The last consideration is a particular concern where an account identifier is exposed to the user. Attempts to 'teach' users to use URIs as account identifiers have been predictably unsuccessful. Users expect and require accounts to be of the form user@example.com and not http://service.example.com/service/user.

The Web Service discovery process described in this specification builds on the approach specified in DNS-Based Service Discovery [RFC6763] . This uses DNS SRV records as the basis for service discovery and TXT records as the basis for service description. This approach allows Web Services to make use of the load balancing and fault tolerance features of SRV and the service negotiation capabilities provided by the service description.

One difficulty that is frequently encountered in attempting to make use of DNS records for service discovery is that it is not always possible for an application process to access this information. Specifications address the world as it actually is rather than as some believe it should be have proven more robust in real world deployment than those that do not. The discovery process defined includes a fallback strategy to enable clients to achieve Web Service discovery in these circumstances.

Another difficulty that is encountered is that the SRV record maps service names to host names rather than Web Service Endpoints. A convention is thus required to map a host name and protocol prefix to a Web Service Endpoint. The HTTP Well Known Service [RFC5785] mechanism is used for this purpose.

While the approach adopted in this specification closely follows that of [RFC6763] , there is an important difference in that the earlier specification sets out a framework which Web Services may apply to develop a discovery approach that suits their particular needs while this specification defines exactly one such approach. In particular, the use of a common set of TXT keys to specify service parameters enables service discovery and negotiation to be delegated to common support libraries rather than being implemented independently in each application.

2. Definitions

This section presents the related specifications and standard, the terms that are used as terms of art within the documents and the terms used as requirements language.

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Defined Terms

Web Service An Internet service provided by one or more Web Service Hosts that are addressable by a single Web Service Endpoint and are intended to provide logically equivalent services.

Web Service Endpoint (WSE) A URI that specifies a Web Service or Web Service Host.

Web Service Host The actual machine (physical or virtual) that provides a Web Service

3. Service Discovery

Service discovery is the process of resolving the address of a Web Service to a Web Service Endpoint, a URI [RFC3986] at which the service is provided.

3.1. Host Identification

The first step in service discovery is to resolve the <domain> and <service> identifiers to the IP address of a host that provides that service.

3.1.1. SRV Host discovery

A client attempting to connect to the service first attempts to locate an SRV record [RFC2782] for the specified service:

_<service>._tcp.<domain> SRV <priority> <weight> <port> <host>

Figure 1

Where <service> is the IANA assigned service name, <priority> and <weight> are the SRV priority and weight parameters specified in [RFC2782] , <port> is the TCP port number and <host> is the DNS name of the host for which the service advertisement is made.

If no SRV records are found, the client MAY abort the connection or attempt use of the Fallback Discovery process described below.

3.2. Service Description

The second step in service discovery is to identify the attributes of the Web Service and Web Service Hosts providing that service.

3.2.1. TXT Service and Host Description

A service MAY advertise service and/or host description information using TXT records as described in DNS-Based Service Discovery [RFC6763] . These have the following format:

```
_<service>._tcp.<domain>  TXT "<key>=<value> [<tag>=<value>]*"
_<service>._tcp.<host>  TXT "<key>=<value> [<tag>=<value>]*"
```

Figure 2

<domain> and <host> are the domain names specified in the corresponding SRV records.

Service descriptions specified under the domain address of the service apply to all host instances of the service. Descriptions specified under the domain address of a host instance apply only to that host instance and take precedence over values specified at the service level.

The following keys are currently defined:

path The path to use to construct the Web Service Endpoint.

version The service version(s) supported in the format <max>-<min>

encoding An IANA media type specifying a supported encoding format

3.3. Service Selection

Web Service Hosts that do not meet the requirements of the client attempting to create a connection are eliminated before applying SRV service selection criteria specified in [RFC2782] .

Clients SHOULD limit the number of connections attempted before abandoning the attempt to connect.

3.4. Web Service Endpoint Determination

Having selected a Web Service Host, the client determines the Web Service Endpoint as follows:

If the description of the host specifies a path key, the corresponding value is used as the path, otherwise,

if the description of the service specifies a path key, the corresponding value is used as the path, otherwise,

the path is /.well-known/srv/<service>

3.5. DNS Fallback

Despite the fact that SRV records have been a part of the DNS standard for 20 years, it is not uncommon for network intermediaries to implement SRV record resolution incorrectly or block it entirely. If no SRV record is found, a client MAY perform fallback discovery if explicitly authorized to do so by the corresponding Web Service protocol specification.

The Web Service Endpoint used is:

https://<service>.<domain>/.well-known/srv/<service>

Figure 3

Fallback discovery constrains the service provider to use a specific DNS configuration and provides inferior load balancing or fault tolerance capabilities to use of SRV records. It does however ensure that the service is reachable in situations where it would otherwise be unavailable.

3.6. Example

The Mathematical Mesh has the Well-Known Service name of ?MMM'. Accounts used in the Mathematical Mesh follow the [RFC5322] format of <user>@<domain>.

Alice has the account alice@example.com and the DNS configuration file for example.com has the following entries:

```
_mmm._tcp.example.com SRV host1.example.com 0 10 80 host1.example.com
_mmm._tcp.example.com SRV host2.example.com 0 40 80 host2.example.com
_mmm._tcp.example.com TXT "version=1.0-2.0"
mmm.example.com       CNAME host3.example.com
host1.example.com     A 10.0.1.1
host2.example.com     A 10.0.1.2
_mmm._tcp.host2.example.com TXT "path=/service"
host3.example.com     A 10.0.1.1
host3.example.com     A 10.0.1.2
```

Figure 4

The client attempts to resolve the address alice@example.com as follows:

1. Client attempts to resolve SRV and TXT records for _mmm._tcp.example.com

2. DNS resolver returns two SRV entries and one TXT entry

3. Client makes a random selection between host1 (20% weighting) and host2 (80% weighting). Chooses host1.

4. Client resolves A/AAAA for host1.example.com and TXT for _mmm._tcp.host1.example.com

5. DNS resolver returns A=10.0.1.1 and TXT=none

6. Client attempts to POST Web Service request to http://host1example.com/.well-known/srv/mmm at host address 10.0.1.1

7. The host at 10.0.1.1 returns 503 Service Unavailable

8. Client resolves A/AAAA for host2.example.com and TXT for _mmm._tcp.host2.example.com

9. DNS resolver returns A=10.0.1.2 and TXT "path=/service"

10. Client attempts to POST Web Service request to http://host2example.com/service at host address 10.0.1.2

11. Request succeeds, session proceeds.

If the same client is used in a network location where the SRV record resolution fails due to a faulty firewall configuration, the resolution proceeds as follows:

1. Client attempts to resolve SRV record for _mmm._tcp.example.com

2. DNS resolver returns ?not found?

3. Client attempts to resolve A and AAAA record

4. DNS resolver returns 10.0.1.1, 10.0.1.2

5. Client makes a random selection between 10.0.1.1 (50% weighting) and 10.0.1.2 (50% weighting). Chooses host1.

6. Client attempts to POST Web Service request to http://example.com/.well-known/srv/mmm at host address 10.0.1.1

7. The host at 10.0.1.1 returns 503 Service Unavailable

8. Client attempts to POST Web Service request to http://example.com/.well-known/srv/mmm at host address 10.0.1.2

9. Request succeeds, session proceeds.

Note that the main differences between these two scenarios is that the use of the SRV record allows the service configuration to account for load balancing with tiers of fallback support and use of service description information while the use of round robin A/AAAA records does not.

4. Further Work

4.1. Additional Description Keys

The use of service and host descriptions to specify security enhancements is currently being considered. This provides a superset of the capabilities specified in [RFC6698] .

Specify minimum TLS version.

Specify trust roots more flexibly

Specify client authentication requirements

Use of security enhancements other than TLS.

Publish public keys to be used to protect negotiation of security enhancements

The use of service and host descriptions to specify use of non-HTTP presentation transports is currently being considered.

4.2. Service Scaling

This document considers the problem of establishing a connection to a Host providing a particular Web Service. When constructing services at very large scale (e.g. millions of concurrent users), it becomes desirable to enable discovery of a Web Service Host responsible for a particular partition of that data (e.g. a particular user account).

Since this is clearly a different problem, it is judged that the best approach is to give it a different name and rule it out of scope of the present work.

5. Security Considerations

A treatment of the security considerations will follow.

6. IANA Considerations

The following registrations are required:

Well-Known URIs /.well-known/srv/

[Or change registry to FCFS]

7. References

7.1. Normative References

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, DOI 10.17487/RFC5785, April 2010.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013.

7.2. Informative References

[RFC5322] Resnick, P., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012.

7.3. URIs

[1] http://mathmesh.com/Documents/draft-hallambaker- web-service-discovery.html

Author's Address

Phillip Hallam-Baker
Comodo Group Inc.

Email: philliph@comodo.com