Internet Engineering Task Force (IETF)
Request for Comments: 6764
Updates: 4791, 6352
Category: Standards Track
ISSN: 2070-1721

C. Daboo
Apple Inc.

February 2013

Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions to WebDAV (CardDAV)

Abstract

This specification describes how DNS SRV records, DNS TXT records, and well-known URIs can be used together or separately to locate CalDAV (Calendaring Extensions to Web Distributed Authoring and Versioning (WebDAV)) or CardDAV (vCard Extensions to WebDAV) services.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6764.

Table of Contents

1. Introduction

[RFC4791] defines the CalDAV calendar access protocol, based on HTTP [RFC2616], for accessing calendar data stored on a server. CalDAV clients need to be able to discover appropriate CalDAV servers within their local area network and at other domains, e.g., to minimize the need for end users to know specific details such as the fully qualified domain name (FQDN) and port number for their servers.

[RFC6352] defines the CardDAV address book access protocol based on HTTP [RFC2616], for accessing contact data stored on a server. As with CalDAV, clients also need to be able to discover CardDAV servers.

[RFC2782] defines a DNS-based service discovery protocol that has been widely adopted as a means of locating particular services within a local area network and beyond, using DNS SRV Resource Records (RRs). This has been enhanced to provide additional service meta-data by use of DNS TXT RRs as per [RFC6763].

This specification defines new SRV service types for the CalDAV protocol and gives an example of how clients can use this together with other protocol features to enable simple client configuration. SRV service types for CardDAV are already defined in Section 11 of [RFC6352].

Another issue with CalDAV or CardDAV service discovery is that the service might not be located at the "root" URI of the HTTP server hosting it. Thus, a client needs to be able to determine the complete path component of the Request-URI to use in HTTP requests: the "context path". For example, if CalDAV is implemented as a "servlet" in a web server "container", the servlet "context path" might be "/caldav/". So the URI for the CalDAV service would be, e.g., "http://caldav.example.com/caldav/" rather than "http://caldav.example.com/". SRV RRs by themselves only provide an FQDN and port number for the service, not a path. Since the client "bootstrapping" process requires initial access to the "context path" of the service, there needs to be a simple way for clients to also discover what that path is.

This specification makes use of the "well-known URI" feature [RFC5785] of HTTP servers to provide a well-known URI for CalDAV or CardDAV services that clients can use. The well-known URI will point to a resource on the server that is simply a "stub" resource that provides a redirect to the actual "context path" resource representing the service endpoint.

2. Conventions Used in This Document

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].

3. CalDAV SRV Service Labels

This specification adds two SRV service labels for use with CalDAV:

_caldav: Identifies a CalDAV server that uses HTTP without Transport Layer Security (TLS) [RFC2818].

_caldavs: Identifies a CalDAV server that uses HTTP with TLS [RFC2818].

Clients MUST honor Priority and Weight values in the SRV RRs, as described by [RFC2782].

Example: service record for server without TLS

```
_caldav._tcp     SRV 0 1 80 calendar.example.com.
```

Example: service record for server with TLS

```
_caldavs._tcp    SRV 0 1 443 calendar.example.com.
```

4. CalDAV and CardDAV Service TXT Records

When SRV RRs are used to advertise CalDAV and CardDAV services, it is also convenient to be able to specify a "context path" in the DNS to be retrieved at the same time. To enable that, this specification uses a TXT RR that follows the syntax defined in Section 6 of [RFC6763] and defines a "path" key for use in that record. The value of the key MUST be the actual "context path" to the corresponding service on the server.

A site might provide TXT records in addition to SRV records for each service. When present, clients MUST use the "path" value as the "context path" for the service in HTTP requests. When not present, clients use the ".well-known" URI approach described next.

Example: text record for service with TLS

```
_caldavs._tcp    TXT path=/caldav
```

5. CalDAV and CardDAV Service Well-Known URI

Two ".well-known" URIs are registered by this specification for CalDAV and CardDAV services, "caldav" and "carddav" respectively (see Section 9). These URIs point to a resource that the client can use as the initial "context path" for the service they are trying to connect to. The server MUST redirect HTTP requests for that resource to the actual "context path" using one of the available mechanisms provided by HTTP (e.g., using a 301, 303, or 307 response). Clients MUST handle HTTP redirects on the ".well-known" URI. Servers MUST NOT locate the actual CalDAV or CardDAV service endpoint at the ".well-known" URI as per Section 1.1 of [RFC5785].

Servers SHOULD set an appropriate Cache-Control header value (as per Section 14.9 of [RFC2616]) in the redirect response to ensure caching occurs or does not occur as needed or as required by the type of response generated. For example, if it is anticipated that the

location of the redirect might change over time, then a "no-cache" value would be used.

To facilitate "context paths" that might differ from user to user, the server MAY require authentication when a client tries to access the ".well-known" URI (i.e., the server would return a 401 status response to the unauthenticated request from the client, then return the redirect response only after a successful authentication by the client).

5.1. Example: Well-Known URI Redirects to Actual "Context Path"

A CalDAV server has a "context path" that is "/servlet/caldav". The client will use "/.well-known/caldav" as the path for its "bootstrapping" process after it has first found the FQDN and port number via an SRV lookup or via manual entry of information by the user, from which the client can parse suitable information. When the client makes an HTTP request against "/.well-known/caldav", the server would issue an HTTP redirect response with a Location response header using the path "/servlet/caldav". The client would then "follow" this redirect to the new resource and continue making HTTP requests there to complete its "bootstrapping" process.

6. Client "Bootstrapping" Procedures

This section describes a procedure that CalDAV or CardDAV clients SHOULD use to do their initial configuration based on minimal user input. The goal is to determine an http: or https: URI that describes the full path to the user's principal-URL [RFC3744].

1. Processing user input:

   * For a CalDAV server:

     + Minimal input from a user would consist of a calendar user address and a password. A calendar user address is defined by iCalendar [RFC5545] to be a URI [RFC3986]. Provided a user identifier and a domain name can be extracted from the URI, this simple "bootstrapping" configuration can be done.

     + If the calendar user address is a "mailto:" [RFC6068] URI, the "mailbox" portion of the URI is examined, and the "local-part" and "domain" portions are extracted.

     + If the calendar user address is an "http:" [RFC2616] or "https:" [RFC2818] URI, the "userinfo" and "host" portion of the URI [RFC3986] is extracted.

* For a CardDAV server:

  + Minimal input from a user would consist of their email address [RFC5322] for the domain where the CardDAV service is hosted, and a password. The "mailbox" portion of the email address is examined, and the "local-part" and "domain" portions are extracted.

2. Determination of service FQDN and port number:

* An SRV lookup for _caldavs._tcp (for CalDAV) or _carddavs._tcp (for CardDAV) is done with the extracted "domain" as the service domain.

* If no result is found, the client can try _caldav._tcp (for CalDAV) or _carddav._tcp (for CardDAV) provided non-TLS connections are appropriate.

* If an SRV record is returned, the client extracts the target FQDN and port number. If multiple SRV records are returned, the client MUST use the Priority and Weight fields in the record to determine which one to pick (as per [RFC2782]).

* If an SRV record is not found, the client will need to prompt the user to enter the FQDN and port number information directly or use some other heuristic, for example, using the extracted "domain" as the FQDN and default HTTPS or HTTP port numbers. In this situation, clients MUST first attempt an HTTP connection with TLS.

3. Determination of initial "context path":

* When an SRV lookup is done and a valid SRV record returned, the client MUST also query for a corresponding TXT record and check for the presence of a "path" key in its response. If present, the value of the "path" key is used for the initial "context path".

* When an initial "context path" has not been determined from a TXT record, the initial "context path" is taken to be "/.well-known/caldav" (for CalDAV) or "/.well-known/carddav" (for CardDAV).

* If the initial "context path" derived from a TXT record generates HTTP errors when targeted by requests, the client SHOULD repeat its "bootstrapping" procedure using the appropriate ".well-known" URI instead.

4. Determination of user identifier:

   * The client will need to make authenticated HTTP requests to the service. Typically, a "user identifier" is required for some form of user/password authentication. When a user identifier is required, clients MUST first use the "mailbox" portion of the calendar user address provided by the user in the case of a "mailto:" address and, if that results in an authentication failure, SHOULD fall back to using the "local-part" extracted from the "mailto:" address. For an "http:" or "https:" calendar user address, the "userinfo" portion is used as the user identifier for authentication. This is in line with the guidance outlined in Section 7. If these user identifiers result in authentication failure, the client SHOULD prompt the user for a valid identifier.

5. Connecting to the service:

   * Subsequent to configuration, the client will make HTTP requests to the service. When using "_caldavs" or "_carddavs" services, a TLS negotiation is done immediately upon connection. The client MUST do certificate verification using the procedure outlined in Section 6 of [RFC6125] in regard to verification with an SRV RR as the starting point.

   * The client does a "PROPFIND" [RFC4918] request with the request URI set to the initial "context path". The body of the request SHOULD include the DAV:current-user-principal [RFC5397] property as one of the properties to return. Note that clients MUST properly handle HTTP redirect responses for the request. The server will use the HTTP authentication procedure outlined in [RFC2617] or use some other appropriate authentication schemes to authenticate the user.

   * If the server returns a 404 ("Not Found") HTTP status response to the request on the initial "context path", clients MAY try repeating the request on the "root" URI "/" or prompt the user for a suitable path.

   * If the DAV:current-user-principal property is returned on the request, the client uses that value for the principal-URL of the authenticated user. With that, it can execute a "PROPFIND" request on the principal-URL and discover additional properties for configuration (e.g., calendar or address book "home" collections).

* If the DAV:current-user-principal property is not returned, then the client will need to request the principal-URL path from the user in order to continue with configuration.

Once a successful account discovery step has been done, clients SHOULD cache the service details that were successfully used (user identity, principal-URL with full scheme/host/port details) and reuse those when connecting again at a later time.

If a subsequent connection attempt fails, or authentication fails persistently, clients SHOULD retry the SRV lookup and account discovery to "refresh" the cached data.

7. Guidance for Service Providers

Service providers wanting to offer CalDAV or CardDAV services that can be configured by clients using SRV records need to follow certain procedures to ensure proper operation.

- CalDAV or CardDAV servers SHOULD be configured to allow authentication with calendar user addresses (just taking the "mailbox" portion of any "mailto:" URI) or email addresses respectively, or with "user identifiers" extracted from them. In the former case, the addresses MUST NOT conflict with other forms of a permitted user login name. In the latter case, the extracted "user identifiers" need to be unique across the server and MUST NOT conflict with any login name on the server.

- Servers MUST force authentication for "PROPFIND" requests that retrieve the DAV:current-user-principal property to ensure that the value of the DAV:current-user-principal property returned corresponds to the principal-URL of the user making the request.

- If the service provider uses TLS, the service provider MUST ensure a certificate is installed that can be verified by clients using the procedure outlined in Section 6 of [RFC6125] in regard to verification with an SRV RR as the starting point. In particular, certificates SHOULD include SRV-ID and DNS-ID identifiers as appropriate, as described in Section 8.

- Service providers should install the appropriate SRV records for the offered services and optionally include TXT records.

8. Security Considerations

Clients that support TLS as defined by [RFC2818] SHOULD try the "_caldavs" or "_carddavs" services first before trying the "_caldav" or "_carddav" services respectively. If a user has explicitly requested a connection with TLS, the client MUST NOT use any service information returned for the "_caldav" or "_carddav" services. Clients MUST follow the certificate-verification process specified in [RFC6125].

A malicious attacker with access to the DNS server data, or that is able to get spoofed answers cached in a recursive resolver, can potentially cause clients to connect to any server chosen by the attacker. In the absence of a secure DNS option, clients SHOULD check that the target FQDN returned in the SRV record matches the original service domain that was queried. If the target FQDN is not in the queried domain, clients SHOULD verify with the user that the SRV target FQDN is suitable for use before executing any connections to the host. Alternatively, if TLS is being used for the service, clients MUST use the procedure outlined in Section 6 of [RFC6125] to verify the service. When the target FQDN does not match the original service domain that was queried, clients MUST check the SRV-ID identifier in the server’s certificate. If the FQDN does match, clients MUST check any SRV-ID identifiers in the server’s certificate or, if no SRV-ID identifiers are present, MUST check the DNS-ID identifiers in the server’s certificate.

Implementations of TLS [RFC5246], used as the basis for TLS ([RFC2818]), typically support multiple versions of the protocol as well as the older SSL (Secure Sockets Layer) protocol. Because of known security vulnerabilities, clients and servers MUST NOT request, offer, or use SSL 2.0. See Appendix E.2 of [RFC5246] for further details.

9. IANA Considerations

9.1. Well-Known URI Registrations

This document defines two ".well-known" URIs using the registration procedure and template from Section 5.1 of [RFC5785].

9.1.1. caldav Well-Known URI Registration

URI suffix: caldav

Change controller: IETF

Specification document(s): This RFC

Related information: See also [RFC4791].

9.1.2. carddav Well-Known URI Registration

URI suffix: carddav

Change controller: IETF

Specification document(s): This RFC

Related information: See also [RFC6352].

9.2. Service Name Registrations

This document registers four new service names as per [RFC6335]. Two are defined in this document, and two are defined in [RFC6352], Section 11.

9.2.1. caldav Service Name Registration

Service Name: caldav

Transport Protocol(s): TCP

Assignee: IESG <iesg@ietf.org>

Contact: IETF Chair <chair@ietf.org>

Description: Calendaring Extensions to WebDAV (CalDAV) - non-TLS

Reference: [RFC6764]

Assignment Note: This is an extension of the http service. Defined TXT keys: path=<context path>

9.2.2. caldavs Service Name Registration

Service Name: caldavs

Transport Protocol(s): TCP

Assignee: IESG <iesg@ietf.org>

Contact: IETF Chair <chair@ietf.org>

Description: Calendaring Extensions to WebDAV (CalDAV) - over TLS

Reference: [RFC6764]

Assignment Note: This is an extension of the https service. Defined TXT keys: path=<context path>

9.2.3. carddav Service Name Registration

Service Name: carddav

Transport Protocol(s): TCP

Assignee: IESG <iesg@ietf.org>

Contact: IETF Chair <chair@ietf.org>

Description: vCard Extensions to WebDAV (CardDAV) - non-TLS

Reference: [RFC6352]

Assignment Note: This is an extension of the http service. Defined TXT keys: path=<context path>

9.2.4. carddavs Service Name Registration

Service Name: carddavs

Transport Protocol(s): TCP

Assignee: IESG <iesg@ietf.org>

Contact: IETF Chair <chair@ietf.org>

Description: vCard Extensions to WebDAV (CardDAV) - over TLS

Reference: [RFC6352]

Assignment Note: This is an extension of the https service. Defined TXT keys: path=<context path>

10. Acknowledgments

This specification was suggested by discussion that took place within the Calendaring and Scheduling Consortium's CalDAV Technical Committee. The author thanks the following for their contributions: Stuart Cheshire, Bernard Desruisseaux, Eran Hammer-Lahav, Helge Hess, Arnaud Quillaud, Wilfredo Sanchez, and Joe Touch.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

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

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC3744] Clemm, G., Reschke, J., Sedlar, E., and J. Whitehead, "Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol", RFC 3744, May 2004.

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

[RFC4791] Daboo, C., Desruisseaux, B., and L. Dusseault, "Calendaring Extensions to WebDAV (CalDAV)", RFC 4791, March 2007.

[RFC4918] Dusseault, L., "HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV)", RFC 4918, June 2007.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[RFC5397] Sanchez, W. and C. Daboo, "WebDAV Current Principal Extension", RFC 5397, December 2008.

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

[RFC6068] Duerst, M., Masinter, L., and J. Zawinski, "The 'mailto' URI Scheme", RFC 6068, October 2010.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, March 2011.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC 6335, August 2011.

[RFC6352] Daboo, C., "CardDAV: vCard Extensions to Web Distributed Authoring and Versioning (WebDAV)", RFC 6352, August 2011.

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

11.2. Informative References

[RFC5545] Desruisseaux, B., "Internet Calendaring and Scheduling Core Object Specification (iCalendar)", RFC 5545, September 2009.

Author's Address

Cyrus Daboo
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
USA

EMail: cyrus@daboo.name
URI: http://www.apple.com/