Network Working Group
Internet-Draft
Updates: XXXX-CardDAV
(if approved)
Intended status: Standards Track
Expires: February 25, 2011

C. Daboo
Apple Inc.

August 24, 2010

CardDAV Directory Gateway Extension
draft-daboo-carddav-directory-gateway-02

Abstract

This document defines an extension to the vCard Extensions to WebDAV (CardDAV) protocol that allows a server to expose a directory as a read-only address book collection.

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 http://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 February 25, 2011.

Copyright Notice

Table of Contents

1. Introduction and Overview

The CardDAV [I-D.ietf-vcarddav-carddav] protocol defines a standard way of accessing, managing, and sharing contact information based on the vCard [RFC2426] format. Often, in an enterprise or service provider environment, a directory of all users hosted on the server (or elsewhere) is available (for example via Lightweight Directory Access Protocol (LDAP) [RFC4510] or some direct database access). It would be convenient for CardDAV clients if this directory were exposed as a "global" address book on the CardDAV server so it could be searched in the same way as personal address books are. This specification defines a "directory gateway" feature extension to CardDAV to enable this.

This specification adds one new WebDAV property to principal resources that contains the URL to one or more directory gateway address book collection resources. It is important for clients to be able to distinguish this address book collection from others because there are specific limitations involved in using it as described below. To aid that, this specification defines an XML element that can be included as a child element of the DAV:resourcetype property of address book collections to identify them as directory gateways.

Note that this feature is in no way intended to replace full directory access - it is meant to simply provide a convenient way for CardDAV clients to query contact-related attributes in directory records.

2. Conventions

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].

The term "protected" is used in the Conformance field of property definitions as defined in Section 15 of [RFC4918].

This document uses XML DTD fragments ([W3C.REC-xml-20081126], Section 3.2) as a purely notational convention. WebDAV request and response bodies cannot be validated by a DTD due to the specific extensibility rules defined in Section 17 of [RFC4918] and due to the fact that all XML elements defined by this specification use the XML namespace name "DAV:". In particular:

1. element names use the "DAV:" namespace,

2. element ordering is irrelevant unless explicitly stated,

3. extension elements (elements not already defined as valid child elements) may be added anywhere, except when explicitly stated otherwise,

4. extension attributes (attributes not already defined as valid for this element) may be added anywhere, except when explicitly stated otherwise.

When XML element types in the namespaces "DAV:" and "urn:ietf:params:xml:ns:carddav" are referenced in this document outside of the context of an XML fragment, the strings "DAV:" and "CARDDAV:" will be prefixed to the element types, respectively.

3. CARDDAV:directory-gateway Property

Name: directory-gateway

Namespace: urn:ietf:params:xml:ns:carddav

Purpose: Identifies URLs of CardDAV address book collections acting as a directory gateway for the server.

Protected: MUST be protected.

allprop behavior: SHOULD NOT be returned by a PROPFIND DAV:allprop request.

Description: The CARDDAV:directory-gateway identifies address book collection resources that are directory gateway address books for the server.

Definition:

```
<!ELEMENT directory-gateway (DAV:href*)>
```

Example:

```
<C:directory-gateway xmlns:D="DAV:"
   xmlns:C="urn:ietf:params:xml:ns:carddav">
  <D:href>/directory</D:href>
</C:directory-gateway>
```

4. XML Element Definitions

4.1. CARDDAV:directory

Name: directory

Namespace: urn:ietf:params:xml:ns:carddav

Purpose: Used to indicate that an address book collection is a directory gateway.

Description: This element appears in the DAV:resourcetype property on a address book collection resources that are directory gateways. Clients can use the presence of this element to identify directory gateway collections when doing PROPFINDs to list collection contents.

Definition:

```
<!ELEMENT directory EMPTY>
```

Example:

```
<D:resourcetype xmlns:D="DAV:"
   xmlns:C="urn:ietf:params:xml:ns:carddav">
  <D:collection/>
  <C:addressbook/>
  <C:directory/>
</D:resourcetype>
```

5. Client Guidelines

Clients wishing to make use of directory gateway address books can request the CARDDAV:directory-gateway property (Section 3) when examining other properties on the principal resource for the user. If the property is not present, then the directory gateway feature is not supported by the server at that time.

Clients can also detect the presence of directory gateway address book collections by retrieving the DAV:resourcetype property on collections that it lists, and look for the presence of the CARDDAV: directory element (Section 4.1).

Since the directory being exposed via a directory gateway address book collection could be large, clients SHOULD limit the number of results returned in an CARDDAV:addressbook-query REPORT as defined in Section 8.6.1 of [I-D.ietf-vcarddav-carddav].

Clients MUST treat the directory gateway address book collection as a read-only collection, so HTTP methods that modify resource data or properties in the address book collection MUST NOT be used.

Clients SHOULD NOT attempt to cache the entire contents of the directory gateway address book collection resource by retrieving all resources, or trying to examine all the properties of all resources (e.g., via a PROPFIND Depth:1 request). Instead, CARDDAV: addressbook-query REPORTs are used to search for specific address book object resources, and CARDDAV:multiget REPORTs and individual GET requests can be made to retrieve the actual vCard data for address book object resources found via a query.

When presenting directory gateway collections to the user, clients SHOULD use the DAV:displayname property on the corresponding address book collections as the name of the directory gateway. This is important in the case where more than one directory gateway is available. Clients MAY also provide descriptive information about each directory gateway by examining the CARDDAV:addressbook-description property (see Section 6.2.1 of [I-D.ietf-vcarddav-carddav]) on the resource.

6. Server Guidelines

Servers wishing to expose a directory gateway as an address book collection MUST include the CARDDAV:directory-gateway property on all principal resources of users expected to use the feature.

Since the directory being exposed via the directory gateway address book collection could be large, servers SHOULD truncate the number of results returned in an CARDDAV:addressbook-query REPORT as defined in Section 8.6.2 of [I-D.ietf-vcarddav-carddav]. In addition, servers SHOULD disallow requests that effectively enumerate the collection contents (e.g., PROPFIND Depth:1, trivial CARDDAV:addressbook-query, DAV:sync-collection REPORT).

Servers need to expose the directory information as a set of address book object resources in the directory gateway address book collection resource. To do that, a mapping between the directory record format and the vCard data has to be applied. In general, only directory record attributes that have a direct equivalent in vCard SHOULD be mapped. It is up to individual implementations to determine which attributes to map. But in all cases servers MUST generate valid vCard data as returned to the client. In addition, as required by CardDAV, the UID vCard property MUST be present in the vCard data, and this value MUST be persistent from query to query for the same directory record.

Multiple directory sources could be available to the server. The server MAY use a single directory gateway resource to aggregate results from each directory source. When doing so care is needed when dealing with potential records that refer to the same entity. Servers MAY suppress any duplicates that they are able to determine themselves. Alternatively, multiple directory sources can be exposed as separate directory gateway resources.

For any directory source, a server MAY expose multiple directory gateway resources where each represents a different query "scope" for the directory. Different scopes MAY be offered to different principals on the server. For example, the server might expose an entire company directory for searching as the resource "/directory-all" to all principals, but then provide "/directory-department-XYZ" as another directory gateway that has a search scope that implicitly limits the search results to just the "XYZ" department. Users in that department would then have a CARDDAV:directory-gateway property on their principal resource that included the "/directory-department-XYZ" resource. Users in other departments would have corresponding directory gateway resources available to them.

Records in a directory can include data for more than just people, e.g, resources such as rooms or projectors, groups, computer systems etc. It is up to individual implementations to determine the most appropriate "scope" for the data returned via the directory gateway by filtering the appropriate record types. As above, servers could choose to expose people and resources under different directory gateway resources by implicitly limiting the search "scope" for each of those.

Servers MAY apply implementation defined access rules to determine, on a per-user basis, what records are returned to a particularly user and the content of those records exposed via vCard data. This per-user behavior is in addition to the general security requirements detailed below.

When multiple directory gateway collections are present, servers SHOULD provide a DAV:displayname property on each that disambiguates them. Servers MAY include a CARDDAV:addressbook-description property (see Section 6.2.1 of [I-D.ietf-vcarddav-carddav]) on each directory gateway resource to provide a description of the directory and any search "scope" that might be used, or any other useful information for users.

7. Security Considerations

Servers MUST ensure that client requests against the directory

gateway address book collection cannot use excessive resources (CPU, memory, network bandwidth etc), given that the directory could be large.

Servers MUST take care not to expose sensitive directory record attributes in the vCard data via the directory gateway address book. In general only those properties that have direct correspondence in vCard SHOULD be exposed.

Servers need to determine whether it is appropriate for the directory information to be available via CardDAV to unauthenticated users. If not, servers MUST ensure that unauthenticated users do not have access to the directory gateway address book object resource and its contents. If unauthenticated access is allowed, servers MAY choose to limit the set of vCard properties that are searchable or returned in the address book object resources when unauthenticated requests are made.

8. IANA Consideration

This document does not require any actions on the part of IANA.

9. Acknowledgments

10. References

10.1. Normative References

[I-D.ietf-vcarddav-carddav]
Daboo, C., "vCard Extensions to WebDAV (CardDAV)", draft-ietf-vcarddav-carddav-10 (work in progress), November 2009.

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

[RFC2426] Dawson, F. and T. Howes, "vCard MIME Directory Profile", RFC 2426, September 1998.

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

[W3C.REC-xml-20081126]
Paoli, J., Yergeau, F., Bray, T., Sperberg-McQueen, C., and E. Maler, "Extensible Markup Language (XML) 1.0 (Fifth

Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <http://www.w3.org/TR/2008/REC-xml-20081126>.

10.2. Informative References

[RFC4510] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

Appendix A. Change History (to be removed prior to publication as an RFC)

Changes in -02

1. Added CARDDAV:directory element for use in DAV:resourcetype

2. Allow CARDDAV:directory-gateway to be multi-valued

3. Explain how a server could implicit "scope" queries on different directory gateway resources

Changes in -01

1. Remove duplicated text in a couple of sections

2. Add example of LDAP/generic database as possible directory "sources"

3. Add text to explain why the client needs to treat this as special and thus the need for a property

4. Added text to server guidelines indicating requirements for handling vCard UID properties

5. Added text to server guidelines explain that different record "types" may exist in the directory and the server is free to filter those as appropriate

6. Added text to server guidelines indicating that server are free to aggregate directory records from multiple sources

7. Added text to server guidelines indicating that servers are free to apply implementation defined access control to the returned data on a per-user basis

Author's Address

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

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