Network Working Group
Request for Comments: 5397
Category: Standards Track

W. Sanchez
C. Daboo
Apple Inc.

December 2008

WebDAV Current Principal Extension

Status of This Memo

Copyright Notice

Abstract

This specification defines a new WebDAV property that allows clients to quickly determine the principal corresponding to the current authenticated user.

Table of Contents

1. Introduction

WebDAV [RFC4918] is an extension to HTTP [RFC2616] to support improved document authoring capabilities. The WebDAV Access Control Protocol ("WebDAV ACL") [RFC3744] extension adds access control capabilities to WebDAV. It introduces the concept of a "principal" resource, which is used to represent information about authenticated entities on the system.

Some clients have a need to determine which [RFC3744] principal a server is associating with the currently authenticated HTTP user. While [RFC3744] defines a DAV:current-user-privilege-set property for retrieving the privileges granted to that principal, there is no recommended way to identify the principal in question, which is necessary to perform other useful operations. For example, a client may wish to determine which groups the current user is a member of, or modify a property of the principal resource associated with the current user.

The DAV:principal-match REPORT provides some useful functionality, but there are common situations where the results from that query can be ambiguous. For example, not only is an individual user principal returned, but also every group principal that the user is a member of, and there is no clear way to distinguish which is which.

This specification proposes an extension to WebDAV ACL that adds a DAV:current-user-principal property to resources under access control on the server. This property provides a URL to a principal resource corresponding to the currently authenticated user. This allows a client to "bootstrap" itself by performing additional queries on the principal resource to obtain additional information from that resource, which is the purpose of this extension. Note that while it is possible for multiple URLs to refer to the same principal resource, or for multiple principal resources to correspond to a single principal, this specification only allows for a single http(s) URL in the DAV:current-user-principal property. If a client wishes to obtain alternate URLs for the principal, it can query the principal resource for this information; it is not the purpose of this extension to provide a complete list of such URLs, but simply to provide a means to locate a resource which contains that (and other) information.

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].

When XML element types in the namespace "DAV:" are referenced in this document outside of the context of an XML fragment, the string "DAV:" will be prefixed to the element type names.

Processing of XML by clients and servers MUST follow the rules defined in Section 17 of WebDAV [RFC4918].

Some of the declarations refer to XML elements defined by WebDAV [RFC4918].

3. DAV:current-user-principal

Name: current-user-principal

Namespace: DAV:

Purpose: Indicates a URL for the currently authenticated user's principal resource on the server.

Value: A single DAV:href or DAV:unauthenticated element.

Protected: This property is computed on a per-request basis, and therefore is protected.

Description: The DAV:current-user-principal property contains either a DAV:href or DAV:unauthenticated XML element. The DAV:href element contains a URL to a principal resource corresponding to the currently authenticated user. That URL MUST be one of the URLs in the DAV:principal-URL or DAV:alternate-URI-set properties defined on the principal resource and MUST be an http(s) scheme URL. When authentication has not been done or has failed, this property MUST contain the DAV:unauthenticated pseudo-principal.

In some cases, there may be multiple principal resources corresponding to the same authenticated principal. In that case, the server is free to choose any one of the principal resource URIs for the value of the DAV:current-user-principal property. However, servers SHOULD be consistent and use the same principal resource URI for each authenticated principal.

COPY/MOVE behavior: This property is computed on a per-request basis, and is thus never copied or moved.

Definition:

```
<!ELEMENT current-user-principal (unauthenticated | href)>
<!-- href value: a URL to a principal resource -->
```

Example:

```
<D:current-user-principal xmlns:D="DAV:">
  <D:href>/principals/users/cdaboo</D:href>
</D:current-user-principal>
```

4. Security Considerations

This specification does not introduce any additional security issues beyond those defined for HTTP [RFC2616], WebDAV [RFC4918], and WebDAV ACL [RFC3744].

5. Acknowledgments

This specification is based on discussions that took place within the Calendaring and Scheduling Consortium's CalDAV Technical Committee. The authors thank the participants of that group for their input.

The authors thank Julian Reschke for his valuable input via the WebDAV working group mailing list.

6. 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.

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

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

Authors' Addresses

Wilfredo Sanchez
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014
USA

EMail: wsanchez@wsanchez.net
URI: http://www.apple.com/

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

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