INTERNET-DRAFT
Intended Category: Informational

Rob Weltman
Mark Smith
Netscape Communications Corp.
Mark Wahl
Sun Microsystems, Inc.
April 2003

LDAP Authorization Identity Request and Response Controls
draft-weltman-ldapv3-auth-response-09.txt

Status of this Memo

Abstract

This document extends the Lightweight Directory Access Protocol (LDAP) [RFC3377] bind [LDAPPROT] operation with a mechanism for requesting and returning the authorization identity it establishes. Specifically, this document defines the Authorization Identity Request and Response controls for use with the Bind operation.

1. Introduction

This document defines support for the Authorization Identity Request Control and the Authorization Identity Response Control for requesting and returning the authorization established in a bind operation. The Authorization Identity Request Control may be submitted by a client in a bind request if authenticating with version 3 of the Lightweight Directory Access Protocol (LDAP) protocol [LDAPv3]. In the LDAP server's bind response, it may then include an Authorization Identity Response Control. The response

control contains the identity assumed by the client. This is useful when there is a mapping step or other indirection during the bind, so

that the client can be told what LDAP identity was granted. Client authentication with certificates is the primary situation where this applies. Also, some Simple Authentication and Security Layer (SASL) authentication mechanisms may not involve the client explicitly providing a DN, or may result in an authorization identity which is different from the authentication identity provided by the client [AUTH].

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" used in this document are to be interpreted as described in [RFCKeyWords].

2. Publishing support for the Authorization Identity Request Control and the Authorization Identity Response Control

Support for the Authorization Identity Request Control and the Authorization Identity Response Control is indicated by the presence of the Object Identifiers (OIDs) 2.16.840.1.113730.3.4.16 and 2.16.840.1.113730.3.4.15, respectively, in the supportedControl attribute [LDAPATTRS] of a server's root DSE.

3. Authorization Identity Request Control

This control MAY be included in any bind request which specifies protocol version 3, as part of the controls field of the LDAPMessage as defined in [LDAPPROT]. In a multi-step bind operation, the client MUST provide the control with each bind request.

The controlType is "2.16.840.1.113730.3.4.16" and the controlValue is absent.

4. Authorization Identity Response Control

This control MAY be included in any final bind response where the first bind request of the bind operation included an Authorization Identity Request Control as part of the controls field of the LDAPMessage as defined in [LDAPPROT].

The controlType is "2.16.840.1.113730.3.4.15". If the bind request succeeded and resulted in an identity (not anonymous), the controlValue contains the authorization identity (authzId), as defined in [AUTH] section 9, granted to the requestor. If the bind request resulted in an anonymous association, the controlValue field is a string of zero length. If the bind request resulted in more than one authzId, the primary authzId is returned in the controlValue field.

The control is only included in a bind response if the resultCode for the bind operation is success.

If the server requires confidentiality protections to be in place prior to use of this control (see Security Considerations), the server reports failure to have adequate confidentiality protections in place by returning the confidentialityRequired result code.

If the client has insufficient access rights to the requested authorization information, the server reports this by returning the insufficientAccessRights result code.

Identities presented by a client as part of the authentication process may be mapped by the server to one or more authorization identities. The bind response control can be used to retrieve the primary authzId.

For example, during client authentication with certificates [AUTH], a client may possess more than one certificate and not be able to determine which one was ultimately selected for authentication to the server. The subject DN field in the selected certificate may not correspond exactly to a DN in the directory, but rather have gone through a mapping process controlled by the server. On completing the certificate-based authentication, the client may issue a SASL [SASL] bind request, specifying the EXTERNAL mechanism and including an Authorization Identity Request Control. The bind response MAY include an Authorization Identity Response Control indicating the DN in the server's DIT which the certificate was mapped to.

5. Alternative Approach with Extended Operation

The LDAP "Who am I?" [AUTHZID] extended operation provides a mechanism to query the authorization identity associated with a bound connection. Using an extended operation as opposed to a bind response control allows a client to learn the authorization identity after the bind has has established integrity and data confidentiality protections. The disadvantages of the extended operation approach are coordination issues between "Who am I?" requests, bind requests, and other requests, and that an extra operation is required to learn the authorization identity. For multithreaded or high bandwidth server application environments, the bind response approach may be preferable.

6. Security Considerations

The Authorization Identity Request and Response Controls are subject to standard LDAP security considerations. The controls may be passed over a secure as well as over an insecure channel. They are not protected by security layers negotiated by the bind operation.

The response control allows for an additional authorization identity to be passed. In some deployments, these identities may contain confidential information which require privacy protection. In such

deployments, a security layer should be established prior to issuing a bind request with an Authorization Identity Request Control.

7. IANA Considerations

The OIDs 2.16.840.1.113730.3.4.16 and 2.16.840.1.113730.3.4.15 are reserved for the Authorization Identity Request and Response Controls, respectively. The Authorization Identity Request Control is to be registered as an LDAP Protocol Mechanism [IANALDAP].

8. Copyright

BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

9. References

[LDAPV3] Hodges, J. and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[LDAPPROT] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFCKeyWords] Bradner, Scott, "Key Words for use in RFCs to Indicate Requirement Levels", draft-bradner-key-words-03.txt, January 1997.

[AUTH] M. Wahl, H. Alvestrand, J. Hodges, RL "Bob" Morgan, "Authentication Methods for LDAP", RFC 2829, May 2000.

[SASL] J. Myers, "Simple Authentication and Security Layer (SASL", RFC 2222, October 1997.

[AUTHZID] K. Zeilenga, "LDAP 'Who am I?' Operation", draft-zeilenga-ldap-authzid-03.txt, April 2002

[LDAPATTRS] M. Wahl, A. Coulbeck, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997

[IANALDAP] J. Hodges, R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002

10. Author's Addresses

Rob Weltman
Netscape Communications Corp.
360 W. Caribbean Drive
Sunnyvale, CA 94089
USA
+1 650 937-3194
rweltman@netscape.com

Mark Smith
Netscape Communications Corp.
360 W. Caribbean Drive
Sunnyvale, CA 94089
USA
+1 650 937-3477
mcs@netscape.com

Mark Wahl
Sun Microsystems, Inc.
911 Capital of Texas Hwy, Suite 4140
Austin, TX 78759
USA
+1 512 231 7224
Mark.Wahl@sun.com