                    Lightweight Directory Access Protocol (LDAP)
                  Authorization Identity Request and Response Controls

Status of this Memo

Copyright Notice

Abstract

   This document extends the Lightweight Directory Access Protocol
   (LDAP) bind 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 DSA-specific Entry (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 may 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.  Upon 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 Directory Information Tree (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 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
   has been registered as an LDAP Protocol Mechanism [IANALDAP].

8.  References

8.1.  Normative References

   [LDAPv3]        Hodges, J. and R. Morgan, "Lightweight Directory Access
                   Protocol (v3): Technical Specification", RFC 3377,
                   September 2002.

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

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

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

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

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

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

8.2.  Informative References

   [AUTHZID]       Zeilenga, K., "LDAP 'Who am I?' Operation", Work in
                   Progress, April 2002.

9.  Author's Addresses

Rob Weltman
America Online
360 W. Caribbean Drive
Sunnyvale, CA 94089
USA

Phone: +1 650 937-3194
EMail: robw@worldspot.com


Mark Smith
Pearl Crescent, LLC
447 Marlpool Drive
Saline, MI 48176
USA

Phone: +1 734 944-2856
EMail: mcs@pearlcrescent.com


Mark Wahl
PO Box 90626
Austin, TX 78709-0626
USA

10.  Full Copyright Statement

Intellectual Property

Acknowledgement