INTERNET-DRAFT Rob Weltman
Intended Category: Standards Track Yahoo!, Inc.
June 2005

LDAP Proxied Authorization Control
draft-weltman-ldapv3-proxy-13.txt

Status of this Memo

Abstract

This document defines the Lightweight Directory Access Protocol (LDAP) Proxy Authorization Control. The Proxy Authorization Control allows a client to request that an operation be processed under a provided authorization identity instead of as the current authorization identity associated with the connection.

1. Introduction

Proxy authorization allows a client to request that an operation be processed under a provided authorization identity instead of as the current authorization identity associated with the connection. This document defines support for proxy authorization using the Control mechanism [RFC 2251]. The Lightweight Directory Access Protocol [LDAPV3] supports the use of the Simple Authentication and Security Layer [SASL] for authentication and for supplying an authorization

identity distinct from the authentication identity, where the authorization identity applies to the whole LDAP session. The Proxy Authorization Control provides a mechanism for specifying an

authorization identity on a per operation basis, benefiting clients that need to efficiently perform operations on behalf of multiple users.

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

2. Publishing support for the Proxy Authorization Control

Support for the Proxy Authorization Control is indicated by the presence of the Object Identifier (OID) "2.16.840.1.113730.3.4.18" in the supportedControl attribute [RFC 2252] of a server's root DSE.

3. Proxy Authorization Control

A single Proxy Authorization Control may be included in any search, compare, modify, add, delete, modify DN or extended operation request message with the exception of any extension that causes a change in authentication, authorization, or data confidentiality [RFC 2829], such as Start TLS [LDAPTLS] as part of the controls field of the LDAPMessage, as defined in [RFC 2251].

The controlType of the proxy authorization control is "2.16.840.1.113730.3.4.18".

The criticality MUST be present and MUST be TRUE. This requirement protects clients from submitting a request that is executed with an unintended authorization identity.

Clients MUST include the criticality flag and MUST set it to TRUE. Servers MUST reject any request containing a Proxy Authorization Control without a criticality flag or with the flag set to FALSE with a protocolError error. These requirements protect clients from submitting a request that is executed with an unintended authorization identity.

The controlValue SHALL be present and contain either an authzId [AUTH] representing the authorization identity for the request or empty if an anonymous association is to be used.

The mechanism for determining proxy access rights is specific to the server's proxy authorization policy.

If the requested authorization identity is recognized by the server, and the client is authorized to adopt the requested authorization identity, the request will be executed as if submitted by the proxy authorization identity, otherwise the result code TBD is returned.

[Note to the IESG/IANA/RFC Editor: the value TBD is to be replaced with an IANA assigned LDAP Result Code (see RFC 3383 section 3.6]

4. Implementation Considerations

One possible interaction of proxy authorization and normal access control is illustrated here for the case of search requests. During evaluation of a search request, an entry which would have been returned for the search if submitted by the proxy authorization identity directly may not be returned if the server finds that the requester does not have the right to assume the requested identity for searching the entry, even if the entry is within the scope of a search request under a base DN which does imply such rights. This means that fewer results, or no results, may be returned compared to the case where the proxy authorization identity issued the request directly. An example of such a case may be a system with fine-grained
access control, where the proxy right requester has proxy rights at the top of a search tree, but not at or below a point or points within the tree.

5. Security Considerations

The Proxy Authorization Control method is subject to general LDAP security considerations [RFC 2251] [AUTH] [LDAPTLS]. The control may be passed over a secure as well as over an insecure channel.

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

Note that the server is responsible for determining if a proxy authorization request is to be honored. "Anonymous" users SHOULD NOT be allowed to assume the identity of others.

6. IANA Considerations

The OID "2.16.840.1.113730.3.4.18" is reserved for the Proxy Authorization Control. It is to be registered as an LDAP Protocol Mechanism [RFC 3383].

A result code for the case where the server does not execute a request using the proxy authorization identity is to be assigned by the IANA.

7. Copyright

8. Normative References

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

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

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

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

[LDAPTLS] J. Hodges, R. Morgan, M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", RFC 2830, May 2000

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

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

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

[RFC 3383] K. Zeilenga, "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", RFC 3383, September 2002

9. Author's Address

Rob Weltman
Yahoo!, Inc
701 First Avenue
Sunnyvale, CA 94089
USA
+1 408 349-5504
robw@worldspot.com

10. Acknowledgements

Mark Smith, formerly of Netscape Communications Corp., Mark Wahl, formerly of Sun Microsystems, Inc, Kurt Zeilenga of OpenLDAP Foundation, Jim Sermersheim of Novell, and Steven Legg of Adacel have contributed with reviews of this document.