INTERNET-DRAFT
Intended Category: Standards Track

Rob Weltman
Netscape Communications Corp.
April 2002

LDAP Proxied Authorization Control
draft-weltman-ldapv3-proxy-10.txt

Status of this Memo

Abstract

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

1. Introduction

This document defines support for proxied authorization using the Control mechanism. LDAP [LDAPV3] supports the use of SASL [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 proposed Proxied 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", "SHOULD", and "MAY" used in this document are to be interpreted as described in [KEYWORDS].

2. Publishing support for the Proxied Authorization Control

Support for the Proxied Authorization Control is indicated by the presence of the OID "2.16.840.1.113730.3.4.18" in the supportedControl attribute of a server's root DSE.

3. Proxied Authorization Control

A single Proxied Authorization Control may be included in any search, compare, modify, add, delete, modDN or extended operation request message (with the exception of any extension that causes a change in authentication, authorization, or data confidentiality [RFC 2828], such as startTLS) as part of the controls field of the LDAPMessage, as defined in [LDAPV3].

The controlType of the proxied 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.

The control value is either an LDAPString [LDAPv3] containing an authzId as defined in section 9 of [AUTH] to use as the authorization identity for the request, or an empty value if the anonymous identity is to be used.

4. Permission to execute as proxy

An LDAP server supporting the Proxied Authorization Control may choose to honor or not honor a particular request. If the control is supported but a particular request is denied, the server MUST return the error code insufficientAccessRights.

The mechanism for determining proxy access rights is server-specific. A typical implementation will evaluate if the requester has proxy access rights at the base DN of the request. If the requester has proxy access rights, and if the authorization identity is recognized by the server, the request will be honored. If the request is honored, it will be executed as if submitted by the proxied authorization identity. The result code TBD is returned if the client is not authorized to adopt the requested authorization identity. [Note to the IESG/IANA/RFC Editor: the value TBD is to be replaced with an IANA assigned LDAP Result Code (see draft-ietf-ldapbis-iana-xx.txt, Section 3.5)]

The interaction of proxied authorization access control 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 proxied authorization identity directly may not be returned if the server finds that the

requester does not have proxy rights to 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 proxied 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 Proxied Authorization Control method is subject to general LDAP security considerations [LDAPV3] [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 proxied authorization request is to be honored. "Anonymous" users SHOULD NOT be allowed to assume the identity of others.

6. 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.

7. Bibliography

[LDAPV3] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[KEYWORDS] 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, R. Morgan, "Authentication Methods for LDAP", RFC 2829, May 2000

[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

8. Author's Address

Rob Weltman
Netscape Communications Corp.
466 Ellis Street
Mountain View, CA 94043
USA
+1 650 937-3194
rweltman@netscape.com

9. Acknowledgements

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

10. Revision History

10.1 Changes from draft-weltman-ldapv3-proxy-09.txt

Removed description of Control mechanism from Abstract.

Added description of how this is different from SASL authz to the Introduction.

Reworded description of the value of the control (no semantic changes).
Added new result code TBD for failure to acquire proxy rights.

Added references to RFCs 2829 and 2830 in Security section.

10.2 Changes from draft-weltman-ldapv3-proxy-08.txt

Proxied Authorization Control

Clarifications: the control may not be submitted with a startTLS request; an empty controlValue implies the anonymous identity; only one control may be included with a request.

Permission to execute as proxy

Replaced "proxy identity" with "proxied authorization identity".

Security Considerations

Added statement that anonymous users should not be allowed to assume the identity of others.

10.3 Changes from draft-weltman-ldapv3-proxy-07.txt

Proxied Authorization Control

Clarification: the content of the control is an LDAPString.

10.4 Changes from draft-weltman-ldapv3-proxy-06.txt

None

10.5 Changes from draft-weltman-ldapv3-proxy-05.txt

The control also applies to add and extended operations.

The control value is an authorization ID, not necessarily a DN.

Confidentiality concerns are mentioned.

10.6 Changes from draft-weltman-ldapv3-proxy-04.txt

The control does not apply to bind, unbind, or abandon operations.

The proxy DN is represented as a string in the control, rather than embedded in a sequence.

Support for the control is published in the supportedControl attribute of the root DSE, not in supportedExtensions.

The security section mentions confidentiality issues with exposing an additional identity.

10.7 Changes from draft-weltman-ldapv3-proxy-03.txt

None

10.8 Changes from draft-weltman-ldapv3-proxy-02.txt

The Control is now called Proxied Authorization Control, rather than Proxied Authentication Control, to reflect that no authentication occurs as a consequence of processing the Control.

Rather than containing an LDAPDN as the Control value, the Control contains a Sequence (which contains an LDAPDN). This is to provide for future extensions.