

LDAP Proxied Authorization Control
draft-weltman-ldapv3-proxy-08.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This document defines support for the Proxied Authorization Control. Controls are an LDAP protocol version 3 extension, to allow passing arbitrary control information along with a standard request to a server, and to receive arbitrary information back with a standard result. 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

Version 3 of the LDAP protocol provides a means of supplying arbitrary additional information along with a request to an LDAP server, and receiving arbitrary additional response information. The Control protocol extension is described in [[LDAPV3](#)], section 4.1.12. This document defines support for proxied authorization using the Control mechanism.

The key words "MUST", "SHOULD", and "MAY" used in this document are to be interpreted as described in [[KEYWORDS](#)].

Expires May 2002

[Page 1]

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

This control may be included in any search, compare, modify, add, delete, modDN or extended operation request message 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 included and MUST be TRUE.

The control value is an LDAPString [[LDAPv3](#)] containing an authzId as defined in section 9 of [[AUTH](#)]. This is the authorization identity to use for the request.

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.

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 proxy identity.

During evaluation of a search request, an entry which would have been returned for the search if submitted by the proxy 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 proxy 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

Expires May 2002

[Page 2]

The Proxied Authorization Control method is subject to standard LDAP security considerations. 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.

6. Copyright

Copyright (C) The Internet Society (date). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING 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

Expires May 2002

[Page 3]

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, and Kurt Zeilenga of OpenLDAP Foundation have contributed with reviews of this draft.

10. Changes from [draft-weltman-ldapv3-proxy-07.txt](#)

Proxied Authorization Control

Clarification: the content of the control is an LDAPString.

11. Changes from [draft-weltman-ldapv3-proxy-06.txt](#)

None

Expires May 2002

[Page 4]

12. 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.

13. 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.

14. Changes from [draft-weltman-ldapv3-proxy-03.txt](#)

None

15. Changes from [draft-weltman-ldapv3-proxy-02.txt](#)**15.1 Renamed Control**

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.

15.2 Control envelope

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.

Expires May 2002

[Page 5]