Network Working Group
INTERNET-DRAFT

Rob Weltman
Netscape Communications Corp.
February 7, 2000

LDAP Proxied Authorization Control
draft-weltman-ldapv3-proxy-04.txt

Status of this Memo

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 connection with sufficient privileges to assume the identity of another entry for the duration of an LDAP request.

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 [1], 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 [2].

2. Publishing support for the Proxied Authorization Control

Support for the Proxied Authorization Control is indicated by the presence of the OID "2.16.840.1.113730.3.4.12" in the supportedExtensions attribute of a server's root DSE.

3. Proxied Authorization Control

This control may be included in any bind, unbind, search, compare, abandon, modify, delete, or modrdn request message as part of the controls field of the LDAPMessage, as defined in [1].

```
proxyAuthControl ::= SEQUENCE {
        controlType     2.16.840.1.113730.3.4.12,
        criticality     BOOLEAN DEFAULT FALSE,
        controlValue    proxyAuthValue
}
```

The criticality MUST be included and MUST be TRUE.

The controlValue contains the BER encoding of a DN used for evaluating the requested rights:

```
proxyAuthValue::= SEQUENCE {
        proxyDN LDAPDN
}
```

It is represented as a Sequence in order to allow future extensions. Implementations MUST return the error code unsupportedCriticalExtension in the event of unrecognized additional elements in the sequence

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 proxy DN corresponds to a valid entry in the directory managed 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

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. No additional confidential information is passed in the control.

Note that the server is responsible for determining if a proxied authorization request is to be honored.

6. Copyright

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

7. Bibliography

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

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

8. Author's Addresses

Rob Weltman
Netscape Communications Corp.
MV-068
501 E. Middlefield Rd.
Mountain View, CA 94043
USA
+1 650 937-3301
rweltman@netscape.com

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

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

10.1 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.

10.2 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.