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 under 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 under the current authorization identity associated with the connection. This document defines support for proxy authorization using the Control mechanism [RFC2251]. 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 perform operations efficiently 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 [RFC2252] of a server's root DSA-specific Entry (DSE).

3. Proxy Authorization Control

A single Proxy Authorization Control may be included in any search, compare, modify, add, delete, or modify Distinguished Name (DN) or extended operation request message. The exception is any extension that causes a change in authentication, authorization, or data confidentiality [RFC2829], such as Start TLS [LDAPTLS] as part of the controls field of the LDAPMessage, as defined in [RFC2251].

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 SHALL either contain an authzId [AUTH] representing the authorization identity for the request or be 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 123 is returned.

4. Implementation Considerations

One possible interaction of proxy authorization and normal access control is illustrated here. During evaluation of a search request, an entry that 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 that does imply
such rights. This means that fewer results, or no results, may be
returned than would be if 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 [RFC2251] [AUTH] [LDAPTLS]. The control may
be passed over a secure channel 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 that requires 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 has been registered as an LDAP Protocol
Mechanism [RFC3383].

A result code (123) has been assigned by the IANA for the case where
the server does not execute a request using the proxy authorization
identity.

7. 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.
8. Normative References


Author’s Address

Rob Weltman
Yahoo!, Inc.
701 First Avenue
Sunnyvale, CA 94089
USA

Phone: +1 408 349-5504
EMail: robw@worldspot.com