Network Working Group
Request for Comments: 3673
Category: Standards Track

K. Zeilenga
OpenLDAP Foundation

December 2003

Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes

Status of this Memo

Copyright Notice

Abstract

The Lightweight Directory Access Protocol (LDAP) supports a mechanism for requesting the return of all user attributes but not all operational attributes. This document describes an LDAP extension which clients may use to request the return of all operational attributes.

1. Overview

X.500 [X.500] provides a mechanism for clients to request all operational attributes be returned with entries provided in response to a search operation. This mechanism is often used by clients to discover which operational attributes are present in an entry.

This documents extends the Lightweight Directory Access Protocol (LDAP) [RFC3377] to provide a simple mechanism which clients may use to request the return of all operational attributes. The mechanism is designed for use with existing general purpose LDAP clients (including web browsers which support LDAP URLs) and existing LDAP APIs.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119].

2. All Operational Attributes

The presence of the attribute description "+" (ASCII 43) in the list of attributes in a Search Request [RFC2251] SHALL signify a request for the return of all operational attributes.

As with all search requests, client implementors should note that results may not include all requested attributes due to access controls or other restrictions. Client implementors should also note that certain operational attributes may be returned only if requested by name even when "+" is present. This is because some operational attributes are very expensive to return.

Servers supporting this feature SHOULD publish the Object Identifier 1.3.6.1.4.1.4203.1.5.1 as a value of the 'supportedFeatures' [RFC3674] attribute in the root DSE.

3. Interoperability Considerations

This mechanism is specifically designed to allow users to request all operational attributes using existing LDAP clients. In particular, the mechanism is designed to be compatible with existing general purpose LDAP clients including those supporting LDAP URLs [RFC2255].

The addition of this mechanism to LDAP is not believed to cause any significant interoperability issues (this has been confirmed through testing). Servers which have yet to implement this specification should ignore the "+" as an unrecognized attribute description per [RFC2251, Section 4.5.1]. From the client's perspective, a server which does not return all operational attributes when "+" is requested should be viewed as having other restrictions.

It is also noted that this mechanism is believed to require no modification of existing LDAP APIs.

4. Security Considerations

This document provides a general mechanism which clients may use to discover operational attributes. Prior to the introduction of this mechanism, operational attributes were only returned when requested by name. Some might have viewed this as obscurity feature. However, this feature offers a false sense of security as the attributes were still transferable.

Implementations SHOULD implement appropriate access controls mechanisms to restricts access to operational attributes.

5. IANA Considerations

This document uses the OID 1.3.6.1.4.1.4203.1.5.1 to identify the feature described above. This OID was assigned [ASSIGN] by OpenLDAP Foundation, under its IANA-assigned private enterprise allocation [PRIVATE], for use in this specification.

Registration of this feature has been completed by IANA [RFC3674], [RFC3383].

Subject: Request for LDAP Protocol Mechanism Registration

Object Identifier: 1.3.6.1.4.1.4203.1.5.1

Description: All Op Attrs

Person & email address to contact for further information:
Kurt Zeilenga <kurt@openldap.org>

Usage: Feature

Specification: RFC3673

Author/Change Controller: IESG

Comments: none

6. Acknowledgment

The "+" mechanism is believed to have been first suggested by Bruce Greenblatt in a November 1998 post to the IETF LDAPext Working Group mailing list.

7. Intellectual Property Statement

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2251] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFC3377] Hodges, J. and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[RFC3674] Zeilenga, K., "Feature Discovery in Lightweight Directory Access Protocol (LDAP)", RFC 3674, December 2003.

8.2. Informative References

[RFC2255] Howes, T. and M. Smith, "The LDAP URL Format", RFC 2255, December 1997.

[RFC3383] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 3383, September 2002.

[X.500] ITU-T Rec. X.500, "The Directory: Overview of Concepts, Models and Service", 1993.

[ASSIGN] OpenLDAP Foundation, "OpenLDAP OID Delegations", http://www.openldap.org/foundation/oid-delegate.txt.

[PRIVATE] IANA, "Private Enterprise Numbers", http://www.iana.org/assignments/enterprise-numbers.

9. Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

10. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.