Network Working Group
Request for Comments: 4529
Category: Standards Track

K. Zeilenga
OpenLDAP Foundation

June 2006

Requesting Attributes by Object Class in the Lightweight Directory Access Protocol (LDAP)

Status of This Memo

Copyright Notice

Abstract

The Lightweight Directory Access Protocol (LDAP) search operation provides mechanisms for clients to request all user application attributes, all operational attributes, and/or attributes selected by their description. This document extends LDAP to support a mechanism that LDAP clients may use to request the return of all attributes of an object class.

Table of Contents

1. Background and Intended Use

In the Lightweight Directory Access Protocol (LDAP) [RFC4510], the search operation [RFC4511] supports requesting the return of a set of attributes. This set is determined by a list of attribute descriptions. Two special descriptors are defined to request all user attributes ("*") [RFC4511] and all operational attributes ("+")

[RFC3673]. However, there is no convenient mechanism for requesting pre-defined sets of attributes such as the set of attributes used to represent a particular class of object.

This document extends LDAP to allow an object class identifier to be specified in attributes lists, such as in Search requests, to request the return of all attributes belonging to an object class. The COMMERCIAL AT ("@", U+0040) character is used to distinguish an object class identifier from an attribute descriptions.

For example, the attribute list of "@country" is equivalent to the attribute list of 'c', 'searchGuide', 'description', and 'objectClass'. This object class is described in [RFC4519].

This extension is intended primarily to be used where the user is in direct control of the parameters of the LDAP search operation, for instance when entering an LDAP URL [RFC4516] into a web browser, such as <ldap:///dc=example,dc=com?@organization?base>.

2. Terminology

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

DSA stands for Directory System Agent (or server).
DSE stands for DSA-specific Entry.

3. Return of All Attributes of an Object Class

This extension allows object class identifiers to be provided in the attributes field of the LDAP SearchRequest [RFC4511] or other request values of the AttributeSelection data type (e.g., attributes field in pre/post read controls [ReadEntry]) and/or <attributeSelector> production (e.g., attributes of an LDAP URL [RFC4516]). For each object class identified in the attributes field, the request is to be treated as if each attribute allowed by that class (by "MUST" or "MAY", directly or by "SUP"erior) [RFC4512] were itself listed.

This extension extends the <attributeSelector> [RFC4511] production as indicated by the following ABNF [RFC4234]:

```
attributeSelector =/ objectclassdescription
objectclassdescription = ATSIGN oid options
ATSIGN = %x40 ; COMMERCIAL AT ("@" U+0040)
```

where <oid> and <options> productions are as defined in [RFC4512].

The <oid> component of an <objectclassdescription> production identifies the object class by short name (descr) or object identifier (numericoid). If the value of the <oid> component is unrecognized or does not refer to an object class, the object class description is to be treated as an unrecognized attribute description.

The <options> production is included in the grammar for extensibility purposes. An object class description with an unrecognized or inappropriate option is to be treated as unrecognized.

Although object class description options and attribute description options share the same syntax, they are not semantically related. This document does not define any object description option.

Servers supporting this feature SHOULD publish the object identifier (OID) 1.3.6.1.4.1.4203.1.5.2 as a value of the 'supportedFeatures' [RFC4512] attribute in the root DSE. Clients supporting this feature SHOULD NOT use the feature unless they know that the server supports it.

4. Security Considerations

This extension provides a shorthand for requesting all attributes of an object class. Because these attributes could have been listed individually, introduction of this shorthand is not believed to raise additional security considerations.

Implementors of this LDAP extension should be familiar with security considerations applicable to the LDAP search operation [RFC4511], as well as with general LDAP security considerations [RFC4510].

5. IANA Considerations

Registration of the LDAP Protocol Mechanism [RFC4520] defined in this document has been completed.

```
Subject: Request for LDAP Protocol Mechanism Registration
Object Identifier: 1.3.6.1.4.1.4203.1.5.2
Description: OC AD Lists
Person & email address to contact for further information:
     Kurt Zeilenga <kurt@openldap.org>
Usage: Feature
Specification: RFC 4529
Author/Change Controller: Kurt Zeilenga <kurt@openldap.org>
Comments: none
```

This OID was assigned [ASSIGN] by OpenLDAP Foundation, under its IANA-assigned private enterprise allocation [PRIVATE], for use in this specification.

6. References

6.1. Normative References

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

[RFC4234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4511] Sermersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006.

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[RFC4516] Smith, M., Ed. and T. Howes, "Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator", RFC 4516, June 2006.

[X.680] International Telecommunication Union - Telecommunication Standardization Sector, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X.680(2002) (also ISO/IEC 8824-1:2002).

6.2. Informative References

[RFC3673] Zeilenga, K., "Lightweight Directory Access Protocol version 3 (LDAPv3): All Operational Attributes", RFC 3673, December 2003.

[RFC4519] Sciberras, A., Ed., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, June 2006.

[RFC4520] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 4520, June 2006.

[ReadEntry] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Read Entry Controls", RFC 4527, June 2006.

[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.

Author's Address

Kurt D. Zeilenga
OpenLDAP Foundation

EMail: Kurt@OpenLDAP.org

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).