STATUS OF THIS MEMO

This document is an Internet-Draft and is in full conformance with all the provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering 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.

This Internet-Draft expires on 20 February 2000. Comments and suggestions on this document are encouraged. Comments on this document should be sent to the LDAPExt working group discussion list: ietf-ldapext@netscape.com or directly to the author.

ABSTRACT

This document describes a control for the Lightweight Directory Access Protocol v3 that is used to return a subset of attribute values from an entry, specifically, only those values that contributed to the search filter evaluating to TRUE.

1. Introduction

When reading an attribute from an entry using LDAP v2 [1] or LDAPv3 [2], it is normally only possible to read either the attribute type, or the attribute type and all its values. It is not possible to selectively read just a few of the attribute values. If an attribute holds many values, for example, the userCertificate attribute, or the subschema publishing operational attributes objectClasses and attributeTypes [3], then it may be desirable for the user to be able to selectively retrieve a subset of the values, specifically, those attributes that match the selection criteria as specified by the user in the filter. This Internet Draft specifies an LDAPv3 control to enable a user to do just that i.e. return only those values that matched (i.e. returned TRUE to) one or more filter items.

The control has been described in such as way as to be compatible with the matchedValuesOnly boolean of the X.500 DAP [4] Search argument.

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 RFC 2119 [5].

2. The matchedValuesOnly Control

The matchedValuesOnly control MAY be critical or non-critical as determined by the user. It is only applicable to the Search operation, and SHALL be ignored by the server if it is present on any other LDAP operation (even if marked critical on such operations).

The object identifier for this control is 1.2.826.0.1.3344810.2.2

The value for this control is a BOOLEAN. An absent value implies FALSE.

The effects of this control on the Search operation are as follows.

i) Every attribute value that evaluates TRUE against one or more filter items, excluding the ignored filter items (see below), is logically marked by the server as contributing to the filter matching.

ii) If the user requests that the contributing attribute types and their values are returned in the Search result (by placing the attribute type in the AttributeDescriptionList, and by setting the typesOnly BOOLEAN to FALSE), then only the attribute values marked as contributing are returned, whilst the other values of the same attribute (if there are any) are not returned.

iii) Attributes that are to be returned to the user, and that have no values marked as contributing, have all their values returned to the user.

iv) Attributes that have values marked as contributing, but which are not asked to be returned to the user, are not returned and the marking is of no practical value.

Certain filters are ignored for the purposes of marking the attribute values as contributing. These are:

the present filter, since this filter does not test against any attribute values;
the equalityMatch filter, since if the user is able to specify the complete attribute value exactly, then there is very little to be gained from having only this value returned;
any negated filter, since this would have the effect of marking all the attribute values except the one(s) that matched the non-negated filter.

Note 1. The inclusion of equalityMatch in the list above maintains compatibility with the X.500 standard.

Note 2. If the equality matching rule does not require the entire attribute value to be presented by the user, then there is something to be gained from asking for this value only to be returned in its entirety. This can be achieved by using the extensibleMatch filter and using the equality matching rule as the matching rule.

3. Security Considerations

This Internet Draft does not discuss security issues at all. Attribute values SHALL only be returned if the access controls applied by the LDAP server allow them to be returned, and in this respect the effect of the matchedValuesOnly control is of no consequence.
4 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.

5. References


6 Authors Address

David Chadwick
IS Institute
University of Salford
Salford
England
M5 4WT

Email: d.w.chadwick@salford.ac.uk