INTERNET-DRAFT
draft-ietf-ldup-subentry-05.txt

Ed Reed
Reed-Matthews, Inc.
November 15, 2000

LDAP Subentry Schema

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all 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 May 15, 2001.

2. Abstract

This document describes an object class called ldapSubEntry which MAY be used to indicate operations and management related entries in the directory, called LDAP Subentries. To control the visibility of entries of type ldapSubEntry, a control, ldapSubentriesControl, is defined, and a special case using Search filters is described.

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 [RFC2119]. The sections below reiterate these definitions and include some additional ones.

3. Definitions

3.1 ldapSubEntry Class

```
( 2.16.840.1.113719.2.142.6.1.1 NAME 'ldapSubEntry'
   DESC 'LDAP Subentry class, version 1'
     SUP top STRUCTURAL
     MAY ( cn ) )
```

The class ldapSubEntry is intended to be used as a super-class when defining other structural classes to be used as LDAP Subentries, and as the structural class to which Auxiliary classes may be added for application specific subentry information. Where possible, the use of Auxiliary classes to extend LDAP Subentries is strongly preferred.

The presence of ldapSubEntry in the list of super-classes of an entry in the directory makes that entry an LDAP Subentry. Object classes derived from ldapSubEntry are themselves considered ldapSubEntry classes, for the purpose of this discussion.

LDAP Subentries MAY be named by their commonName attribute [RFC2251]. Other naming attributes are also permitted.

LDAP Subentries MAY be containers, unlike their [X.501] counterparts.

LDAP Subentries MAY be contained by, and will usually be located in the directory information tree immediately subordinate to, administrative points. Further (unlike **X.500 subentries), LDAP Subentries MAY be contained by** other LDAP Subentries (the way organizational units may be contained by other organizational units). Deep nestings of LDAP Subentries are discouraged, but not prohibited.

3.2 ldapSubentriesControl

This control is included in the searchRequest message as part of the controls field of the LDAPMessage, as defined in Section 4.1.12 of [RFC2251].

The controlType is set to "1.3.6.1.4.1.7628.5.101.1". The criticality MAY be set to either TRUE or FALSE. The

controlValue is absent.

There is no corresponding response control defined.

LDAP servers that support this control MUST treat LDAP Subentries as "operational objects" in much the same way that "operational attributes" are not returned in search results and [X.511] read operations when only user attributes are requested.

Entries which are not LDAP Subentries may still be referenced in the base object of search operations where the ldapSubentriesControl is present in the request.

3.2.1 LDAP Search with scope other than baseObject

The ldapSubentriesControl is defined for LDAP to signal to LDAP Search operations that ONLY LDAP Subentries are to be included in the return set of entries for the Search, provided other Search criteria (such as scope and filter) are satisfied. When ldapSubentriesControl is NOT included in a Search request on a server that supports the control, LDAP Subentries MUST be omitted from the return set (with the single exception described in section 3.3, below).

3.2.2 LDAP Search with scope of baseObject

For Search operations with a scope value of baseObject, the presence or absence of the ldapSubentriesControl MUST be ignored. Specifically, baseObject searches applied to ldapSubEntry entries MUST be evaluated by Search as if the ldapSubentriesControl is present, even if it is absent.

This provision is intended to preserve the behavior of [X.511] Read operations, which are not affected by the [X.511] subentries control (see section 3.2.4 below), and because it would seem silly to behave otherwise.

3.2.3 Other LDAP operations

The ldapSubentriesControl is not defined for any LDAP operation other than Search. However, an LDAPv3 Extension MAY define a use of this control with that extension as long as such use is consistent with this specification.

3.2.4 Correspondence to X.500 [X.511]

In [X.511] a ServiceControl option is used to govern the visibility of [X.501] subentries. The subentry ServiceControl option is a specific bit of a bitstring that, when set to TRUE in the common arguments of an X.500 Search or List operation, indicates that the operation is to access ONLY the subentries found in the context of the list or search. In fact, normal entries are explicitly NOT returned in the result of a list or search operation when the X.500 subentries ServiceControl is set.

Entries which are not subentries may still be referenced in the base object of list and search operations where the subentries control is set.

The [X.511] subentries ServiceControl has no meaning for operations other than Search and List (i.e., Read, Modify, Delete, etc.).

3.3 Search Filter

LDAP servers MUST implement the following special handling of ldapSubEntry entries: search operations which include a filter "objectclass=ldapSubEntry" MUST include entries derived from the ldapSubEntry class in the scope of their operations, regardless of whether the control (section 3.2 above) is included in the Search or not.

This method of requesting the operation be applied to entries of ldapSubEntry class is intuitive, and is specified to maintain consistency with previous drafts of this document.

Developers SHOULD use the control (section 3.2) in lieu of the Search Filter method of searching for LDAP Subentries, as the Search Filter method MAY be depreciated in the future.

4. Security Considerations

LDAP Subentries will frequently be used to hold data which

reflects either the actual or intended behavior of the directory service. As such, permission to read such entries MAY need to be restricted to authorized users.

More importantly, IF a directory service treats the information in an LDAP Subentry as the authoritative source of policy to be used to control the behavior of the directory, then permission to create, modify, or delete such entries MUST be carefully restricted to authorized administrators.

5. References

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

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

[X.501] ITU-T Rec. X.501, "The Directory: Models", 1993 and subsequent versions

[X.511] ITU-T Rec. X.501, "The Directory: Abstract Service Definition", 1993 and subsequent versions

6. Copyright Notice

7. Acknowledgements

The use of subEntry object class to store Replica and Replication Agreement information is due primarily to the lucid explanation by Mark Wahl, (then of Innosoft), of how they could be used and extended.

8. Author's Address

Edwards E. Reed
Reed-Matthews, Inc.
1064 E 140 North

Lindon, UT 84042
USA
E-mail: eer@oncalldba.com

LDUP Mailing List: ietf-ldup@imc.org
LDAPEXT Mailing List: ietf-ldapext@netscape.com

Expires May 15, 2001