

Network Working Group
Internet-Draft
Expires: March 16, 2008

A. Findlay
Skills 1st Ltd
September 13, 2007

The LDAP groupOfEntries object class
draft-findlay-ldap-groupofentries-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on March 16, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This memo describes the LDAP groupOfEntries object class which is a replacement for the existing groupOfNames class. The new class permits the creation of empty groups.

If approved as a Standards Track document, this document will update [RFC4519](#) [2]

Document Intent

This document is intended to be, after appropriate review and revision, submitted to the RFC Editor as a Standards Track document.

Distribution of this memo is unlimited. Technical discussion of this document will take place on the IETF LDAP Extensions mailing list <ldapext@ietf.org>. Please send editorial comments directly to the author <andrew.findlay@skills-1st.co.uk>

1. Introduction

A groupOfNames object class has existed since the earliest X.521 [[1](#)] standard. It has an identical definition in LDAP ([RFC4519](#) [[2](#)]). The class is used to define entries holding DN-valued member attributes, each value pointing to an entry that represents a single member of the group being described, or to another entry of type groupOfNames.

groupOfNames is a structural object class, so it is often the only class used in the definition of group objects.

Experience has shown that the definition of groupOfNames causes difficulties in practice. In particular, the fact that 'member' is a mandatory attribute means that it is not possible to create an empty group or to delete the last member from a group. This leads to artificial tricks such as making every group a member of itself, or adding a dummy member to every group when it is created. These tricks in turn make the management of groups more complex and prone to error. Groups are commonly used to control access to resources, so management errors can lead to security risks.

There does not appear to be any good reason for the 'member' attribute to be mandatory. This memo describes a new object class called groupOfEntries that is equivalent to groupOfNames in all other respects but which makes 'member' an optional attribute.

2. The existing groupOfNames object class

[RFC4519](#) [[2](#)] contains this definition:

The 'groupOfNames' object class is the basis of an entry that represents a set of named objects including information related to the purpose or maintenance of the set. (Source: X.521 [[1](#)])

```
( 2.5.6.9 NAME 'groupOfNames'
  SUP top
  STRUCTURAL
  MUST ( member $
        cn )
  MAY ( businessCategory $
        seeAlso $
        owner $
        ou $
        o $
```

```
description ) )
```

The inclusion of 'member' in the 'MUST' section of the definition prevents empty groups from being created.

3. The groupOfEntries object class

The 'groupOfEntries' object class is the basis of an entry that represents a set of named objects including information related to the purpose or maintenance of the set. It should be used in preference to the 'groupOfNames' object class.

```
( 1.2.826.0.1.3458854.2.1.1.1 NAME 'groupOfEntries'  
  SUP top  
  STRUCTURAL  
  MUST ( cn )  
  MAY ( member $  
        businessCategory $  
        seeAlso $  
        owner $  
        ou $  
        o $  
        description ) )
```

This object class allows groups to be empty. In all other respects it behaves like the groupOfNames object class.

The OID assigned to this object class is delegated by Skills 1st Ltd.

4. Effect on other documents

This draft deprecates the use of the groupOfNames object class in [RFC4519](#) [2] and replaces it with the groupOfEntries class.

5. IANA considerations

It is requested that IANA register upon Standards Action the groupOfEntries Object Identifier Descriptor and its associated OID.

6. Security considerations

Groups are commonly used to define access permissions to directory entries and resources in other services. Allowing for empty groups avoids the risks associated with leaving a dummy placeholder member in group entries, so security is improved.

[Appendix A](#). Acknowledgements

The author gratefully acknowledges the contributions of Michael Stroeder to the first draft of this document.

[7](#). Informative References

- [1] "The Directory: Selected Object Classes", ITU-T Recommendation X.521, March 1988.
- [2] "LDAP: Schema for User Applications", [RFC 4519](#), June 2006.

Author's Address

Andrew Findlay
Skills 1st Ltd
2 Cedar Chase
Taplow
Maidenhead SL6 0EU
GB

Phone: +44 1628 782565
Email: andrew.findlay@skills-1st.co.uk
URI: <http://www.skills-1st.co.uk/>

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights

might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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