Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 11, 2013

M. Stroeder

January 7, 2013

Lightweight Directory Access Protocol (LDAP): Structural Object Classes for Named Objects
draft-stroeder-namedobject-01

Abstract

This document defines structural object classes that can be used when no other structural object class seems suitable. Especially the object classes will give the possibility to associate a common name and a free-form description with the object.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Standards for LDAP directories often define additional schema elements, especially auxiliary object classes that are intended to hold various attributes needed by that standard. When adding entries with such an auxiliary object class it is up to the directory operator to choose an appropriate structural object class required to add the entry. Often the structural object classes used were defined for other purposes and thus seem too complex for this simple purpose.

Inspired by unfinished [I-D.howard-namedobject] this document defines structural object classes, 'namedObject' and 'namedPolicy'. Only attributes defined in [RFC4519] and [RFC4524] are used within these simple object classes. Arbitrary auxiliary object classes may be thus associated with entries which have such a structural object class.

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].

This document is being discussed on the ldapext@ietf.org mailing list.

2. Object Class Definitions

The object classes definitions in this section are using the attributes 'cn' and 'description' defined in [RFC4519] and 'uniqueIdentifier' defined in [RFC4524].

If the optional attribute 'uniqueIdentifier' contains a value it SHOULD be used to form the RDN of the entry. Otherwise the mandantory attribute 'cn' SHOULD be used to form the RDN of the entry if there are no other appropriate naming attributes available. Other attributes allowed by auxiliary classes also MAY be used for naming purposes.

LDAP clients displaying a list of entries of these object classes SHOULD use mandantory attribute 'cn' to display select lists, hyper-links etc.

2.1. 'namedObject'

The 'namedObject' object class definition is the basis of an entry that represents an arbitrary named object. The attribute 'cn' MUST be added to the entry. The attributes 'uniqueIdentifier' and 'description' MAY be added to the entry.

```
( 1.3.6.1.4.1.5427.1.389.6.20
  NAME 'namedObject'
  SUP top
  STRUCTURAL
  MUST cn
  MAY ( uniqueIdentifier $ description ) )
```

2.2. 'namedPolicy'

The 'namedPolicy' object class definition is sub-classed from 'namedObject'. It SHOULD only be used for entries which represents an arbitrary policy. A typical example would be to use it along with auxiliary object class 'pwdPolicy' defined in [I-D.behera-ldap-password-policy].

The rationale for an extra structural object class is to have the possibility to associate a specific set of policy-related auxiliary object classes without having to restrict the more general 'namedObject' class.

```
( 1.3.6.1.4.1.5427.1.389.6.21
  NAME 'namedPolicy'
  SUP namedObject
  STRUCTURAL )
```

3. Acknowledgements

The 'namedObject' object class definition in this document supersedes the specification of the 'namedObject' in [I-D.howard-namedobject] by L. Howard.

4. IANA Considerations

The OID arc used for the object class defintions is:
iso(1) org(3) dod(6) internet(1) private(4) enter-prise(1)
stroeder.com(5427) public(1) ldap(389) objectClasses(6)

5. Security Considerations

The introduction of these object classes does not impact the security of the Internet or a particular LDAP directory service.

Security considerations for LDAP in general are discussed in documents comprising the technical specification [RFC4510].

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.

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

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

[RFC4524] Zeilenga, K., "COSINE LDAP/X.500 Schema", RFC 4524, June 2006.

6.2. Informative References

[I-D.behera-ldap-password-policy]
Sermersheim, J., Poitou, L., and H. Chu, "Password Policy for LDAP Directories", draft-behera-ldap-password-policy-10 (work in progress), August 2009.

[I-D.howard-namedobject]
Howard, L., "A Structural Object Class for Arbitrary Auxiliary Object Classes", draft-howard-namedobject-00 (work in progress), June 2002.

Author's Address

Michael Stroeder
Karlsruhe
Germany

Email: michael@stroeder.com
URI: http://www.stroeder.com