Internet2 Middleware Initiative
Internet2 Document

K. Hazelton for MACE-Dir
University of Wisconsin-Madison

July 5, 2005

# LDAP representations of membership in groups

## internet2-mace-dir-ldap-group-membership-200507.html

## Status of this Memo

This document is an Internet2 Document and is in compliance with relevant Internet2 document standards.

Internet2 Documents are working documents of Internet2, its areas, and its working groups.

This document is a submission from the **MACE-Dir WG** of the Internet2 **Middleware Initiative**. Comments should be sent to **mace-dir-comments at internet2.edu**.

### Abstract

There are a growing number of situations where a standardized representation of group memberships would help support interoperation between multiple processes and systems. The Internet2 Middleware Initiative projects **Grouper** and **Signet** are two cases in point. This document proposes a recommended binding for "isMemberOf" and "hasMember" to the LDAP protocol.

### 1. Context

This document specifies two ways to represent the association between an entity and a group sketched in "Group and Membership Concepts [1]. It defines an "isMemberOf" attribute that can be carried in an entity's entry in an LDAP directory and a "hasMember" attribute that can be carried in a group's entry in an LDAP directory.

### 2. Specification

### 2.1 eduMember Object Class

```
objectclasses: ( 1.3.6.1.4.1.5923.1.5.2.1
NAME 'eduMember'
AUXILIARY
MAY ( isMemberOf $ hasMember )
)
```

An auxiliary object class, "eduMember," is a convenient container for an extensible set of attributes concerning group memberships. At this time, the only attributes specified as belonging to the the object class are "isMemberOf" and "hasMember."

### 2.2 isMemberOf Attribute

An "isMemberOf" attribute associated with an entity is a collection of values each of which identifies a group in which that entity is a member.

```
attributetypes: ( 1.3.6.1.4.1.5923.1.5.1.1
NAME 'isMemberOf'
DESC 'identifiers for groups to which containing entity belongs'
EQUALITY caseExactMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

**Application utility class**: standard; **# of values**: multi

**Definition**

The values of isMemberOf are identifiers for groups to which the containing entity belongs

**Permissible values** (if controlled)

Any string. If the context requires global uniqueness, well-formed URIs are recommended.

**Notes**

IsMemberOf is defined as an optional (MAY) attribute in the auxiliary object class "eduMember". This means that the attribute can be added to any entry, regardless of that entity's structural object class as long as eduMember is defined in the directory schema.

**Semantics**

The presence of a group identifier as a value of "ismemberOf" implies that the containing entity is a member of the identified group.

**Example applications for which this attribute would be useful**

controlling access to resources

**Example** (LDIF Fragment)

isMemberOf: Stanford:faculty:emeritus

**Syntax**: directoryString; **Indexing**: pres,eq

---

### 2.3 hasMember Attribute

A "hasMember" attribute associated with a group is a collection of values each of which identifies an entity that belongs to the group.

```
attributetypes: ( 1.3.6.1.4.1.5923.1.5.1.2
NAME 'hasMember'
DESC 'identifiers for entities that are members of the group'
EQUALITY caseExactMatch
SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

**Application utility class**: standard; **# of values**: multi

**Definition**

The values of hasMember are identifiers for entities that are members of the group in whose entry this attribute occurs

**Permissible values** (if controlled)

Any string. If the context requires global uniqueness, well-formed URIs are recommended.

**Notes**

The hasMember attribute is defined here to provide a new method for representing the set of entities belonging to a given group. Presence of an entity identifier as a value of "hasMember" implies that the containing group has that entity as a member. Note: this specification does not make any assumptions about how groups are represented in an LDAP directory. There are any number of ways, and these vary across vendors and implementations. HasMember is defined as an optional (MAY) attribute in the auxiliary object class "eduMember". This means that the attribute can be added to any entry, regardless of that entity's structural object class as long as eduMember is defined in the directory schema.

Other long-standing methods for representing group membership, such as groupOfNames, have deeply ingrained patterns of usage and are somewhat restrictive in their definitions: for example, the values of the member attribute for groupOfNames must be given as DNs. The needs arising from the Grouper and Signet projects of Internet2 MACE provided the motivation for defining a new attribute and specifying its syntax and semantics in a way that met those middleware services' need for flexibility and extensibility.

**Semantics**

The presence of an entity identifier as a value of "hasMember" implies that the containing group has that entity as a member.

**Example applications for which this attribute would be useful**

controlling access to resources

**Example** (LDIF Fragment)

hasMember: 5433EF3A-6B65-F701-CE21-FEFF47908173
This example shows a user being represented by her unique person registry identifier in UUID syntax rather than the more familiar DN or a UID.

**Syntax**: directoryString; **Indexing**: pres,eq

### 3. References

[1] Group and membership concepts

### 4. Change Log

[1] Error correction: "draft" changed to "document" in Abstract

## Author's Contact Information

Keith Hazelton
University of Wisconsin-Madison
1210 W. Dayton St.
Madison, WI 53706
US
**Phone:** +1 608 262 0771
**EMail:** hazelton@doit.wisc.edu