

---

# draft-findlay-ldap-groupofentries

## ObjectClass groupOfEntries

Une classe objet groupOfNames existe depuis le standard X.521. Il a une définition identique dans LDAP (rfc4519). La classe est utilisée pour définir des entrées contenant des attributs de DN de membres, chaque valeur pointant vers une entrée qui représente un simple membre du groupe décrit, ou vers une autre entrée de type groupOfNames.

groupOfNames est une classe structurelle, donc elle est souvent la seulement utilisé dans la définition des objets groupes.

L'expérience a montré que la définition des groupOfNames créé des difficultés en pratique. En particulier, le fait que 'member' est un attribut mandatoire signifie qu'il n'est pas possible de créer un groupe vide ou de supprimer le dernier membre d'un groupe. Cela impose certains artifices tels que créer un groupe membre de lui-même, ou d'ajouter un faux membre quand un groupe est créé. Cela rend la gestion des groupes plus complexe et sujet à erreurs. Les groupes sont communément utilisés pour contrôler l'accès aux ressources, dont les erreurs de gestion peuvent conduire à des risques de sécurité.

Il n'y a pas de raison apparente pour que l'attribut 'member' soit mandatoire. Ce mémo décrit une nouvelle classe appelée groupOfEntries qui est équivalent à groupOfNames à l'exception de l'attribut 'member' qui est optionnel.

## Définition

La classe groupOfEntries est la base d'une entrée qui représente un jeu d'objets nommés incluant des informations liées à l'objectif ou la maintenance du jeu. Elle devrait être utilisée de préférence à groupOfNames :

```
( 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 ) )
```

## Effets sur d'autres documents

Ce draft déprécie l'utilisation de groupOfNames dans la rfc4519 et le remplace par la classe groupOfEntries.