

Groupe de travail Réseau
Request for Comments : 3671
 Catégorie : Sur la voie de la normalisation

K. Zeilenga, OpenLDAP Foundation
 décembre 2003
 Traduction Claude Brière de L'Isle

Attributs collectifs dans le protocole léger d'accès à un répertoire (LDAP)

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de Copyright

Copyright (C) The Internet Society (2003). Tous droits réservés.

Résumé

Les attributs collectifs de la Recommandation UIT-T X.500 permettent de partager des caractéristiques communes entre des collections d'entrées. Le présent document résume le modèle d'informations de X.500 pour les attributs collectifs et décrit l'utilisation des attributs collectifs dans le protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*). Le présent document donne les définitions de schéma pour les attributs collectifs à utiliser dans LDAP.

Table des matières

1. Introduction.....	2
1.1 Collections d'entrées.....	2
1.2 Attributs collectifs.....	2
1.3 Conventions.....	2
2. Schéma de système pour les attributs collectifs.....	2
2.1 collectiveAttributeSubentry.....	2
2.2 collectiveAttributeSubentries.....	3
2.3 collectiveExclusions.....	3
3. Types d'attribut Collectifs.....	3
3.1 Nom localement collectif.....	3
3.2 Nom collectifs dans un pays ou province.....	3
3.3 Adresse de rue collective.....	4
3.4 Nom d'organisation collective.....	4
3.5 Nom d'unité organisationnelle collective.....	4
3.6 Adresse postale collective.....	4
3.7 Code postal collectif.....	4
3.8 Boîte postale collective.....	4
3.9 Nom de bureau de livraison physique collectif.....	4
3.10 Numéro de téléphone collectif.....	4
3.11 Numéro de télex collectif.....	4
3.13 Numéro de télécopie collectif.....	5
3.14 Numéro RNIS international collectif.....	5
4. Considérations sur la sécurité.....	5
5. Considérations relatives à l'IANA.....	5
6. Déclaration de propriété intellectuelle.....	6
7. Remerciements.....	6
8. Références.....	6
8.1 Références normatives.....	6
8.2 Références pour information.....	6
9. Adresse de l'auteur.....	7
10. Déclaration complète de droits de reproduction.....	7

1. Introduction

Dans [X.500], un attribut collectif est "un attribut d'utilisateur dont les valeurs sont les mêmes pour chaque membre d'une collection d'entrées" [X.501]. Le présent document détaille leur utilisation dans le protocole léger d'accès à un répertoire (LDAP) [RFC3377].

1.1 Collections d'entrées

Une collection d'entrées est un groupement d'entrées d'objets et d'alias fondé sur des propriétés commune ou des relations partagées entre les entrées correspondantes qui partagent certains attributs. Une collection d'entrées consiste en toutes les entrées dans la portée d'une sous entrée d'attributs collectifs [RFC3672]. Une entrée peut appartenir à plusieurs collections d'entrées.

1.2 Attributs collectifs

Les attributs partagés par les entrées composant une collection d'entrée sont appelés des attributs collectifs. Les valeurs des attributs collectifs sont visibles mais ne peuvent pas être mises à jour par les clients qui accèdent aux entrées dans la collection. Les attributs collectifs sont mis à jour (c'est-à-dire, modifiés) via leur sous entrée d'attribut collectif associée.

Quand une entrée appartient à plusieurs collections d'entrées, les valeurs d'entrée de chaque attribut collectif sont combinées de telle sorte que les sources indépendantes de ces valeurs ne sont pas montrées aux clients.

Les entrées peuvent spécifiquement exclure un attribut collectif particulier en faisant la liste des attributs comme une valeur de l'attribut collectiveExclusions. Comme les autres attributs d'utilisateur, les attributs collectifs sont soumis à divers contrôles incluant des contrôles d'accès, administratifs, et de contenu.

1.3 Conventions

Les définitions de schémas sont fournies en utilisant les formats de description LDAPv3 [RFC2251], [RFC2252]. Les définitions fournies ici sont formatées (saut à la ligne) pour la lisibilité.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Schéma de système pour les attributs collectifs

Les attributs opérationnels suivants sont utilisés pour gérer les attributs collectifs. Les serveurs LDAP [RFC3377] DOIVENT agir conformément aux modèles de répertoire X.500 [X.501] lorsque ils fournissent ce service.

2.1 collectiveAttributeSubentry

Les sous entrées de cette classe d'objet sont utilisées pour administrer les attributs collectifs et sont appelées des sous entrées d'attribut collectif.

(2.5.17.2 NAME 'collectiveAttributeSubentry' AUXILIARY)

Une sous entrée d'attribut collectif DEVRAIT contenir au moins un attribut collectif. Les attributs collectifs contenus dans une sous entrée d'attribut collectif sont disponibles pour trouver, chercher, et faire des comparaisons à chaque entrée dans la portée de cette sous entrée. Les attributs collectifs sont cependant administrés (par exemple, modifiés) via la sous entrée.

Les mises en œuvre de la présente spécification DEVRAIENT prendre en charge les sous entrées d'attribut collectif dans les deux zones administratives collectiveAttributeSpecificArea (2.5.23.5) et collectiveAttributeInnerArea (2.5.23.6) [RFC3672], [X.501].

2.2 collectiveAttributeSubentries

L'attribut opérationnel collectiveAttributeSubentries identifie toutes les sous entrées d'attribut collectif qui affectent l'entrée.

```
( 2.5.18.12 NAME 'collectiveAttributeSubentries'
  EQUALITY distinguishedNameMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
  USAGE directoryOperation NO-USER-MODIFICATION )
```

2.3 collectiveExclusions

L'attribut opérationnel collectiveExclusions permet à des attributs collectifs particuliers d'être exclus d'une entrée. Il PEUT apparaître dans toute entrée et PEUT avoir plusieurs valeurs.

```
( 2.5.18.7 NAME 'collectiveExclusions'
  EQUALITY objectIdentifierMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
  USAGE directoryOperation )
```

Le descripteur excludeAllCollectiveAttributes est associé à l'OID 2.5.18.0. Quand ce descripteur ou OID est présent comme valeur de l'attribut collectiveExclusions, tous les attributs collectifs sont exclus d'une entrée.

3. Types d'attribut Collectifs

Un type d'attribut userApplications peut être défini comme étant COLLECTIVE [RFC2252]. Cela indique que les mêmes valeurs d'attribut vont apparaître dans les entrées d'une collection d'entrées soumise à l'utilisation de l'attribut collectiveExclusions et d'autres contrôles administratifs. Ces contrôles administratifs PEUVENT inclure des règles de contenu de DIT, si elles sont mises en œuvre.

Les types d'attributs collectifs sont couramment définis comme des sous types de types non d'attribut collectif. Par convention, les attributs collectifs sont désignés en mettant en préfixe de nom de leur super type non collectif "c-". Par exemple, l'attribut collectif téléphone est appelé c-TelephoneNumber d'après son super type non collectif telephoneNumber.

Les types d'attributs non collectifs NE DEVRONT PAS avoir de sous type d'attribut collectif.

Les attributs collectifs NE DEVRONT PAS être d'une seule valeur. Les types d'attributs collectifs NE DEVRONT PAS apparaître dans les types d'attribut d'une définition de classe d'objet.

Les attributs opérationnels NE DEVRONT PAS être définis comme collectifs.

Le reste de cette section donne un résumé des attributs collectifs dérivé de celui défini dans [X.520]. Le type d'attribut SUPerior est décrit dans la [RFC2256] pour son utilisation avec LDAP.

Les mises en œuvre de la présente spécification DEVRAIENT prendre en charge les attributs collectifs suivants et PEUVENT prendre en charge des attributs collectifs supplémentaires.

3.1 Nom localement collectif

Le type d'attribut c-l spécifie un nom de localité pour une collection d'entrées.

```
( 2.5.4.7.1 NAME 'c-l' SUP l COLLECTIVE )
```

3.2 Nom collectifs dans un pays ou province

Le type d'attribut c-st spécifie un nom de pays ou province pour une collection d'entrées.

```
( 2.5.4.8.1 NAME 'c-st' SUP st COLLECTIVE )
```

3.3 Adresse de rue collective

Le type d'attribut c-street spécifie une adresse de rue pour une collection d'entrées.

(2.5.4.9.1 NAME 'c-street' SUP street COLLECTIVE)

3.4 Nom d'organisation collective

Le type d'attribut c-o spécifie un nom d'organisation pour une collection d'entrées.

(2.5.4.10.1 NAME 'c-o' SUP o COLLECTIVE)

3.5 Nom d'unité organisationnelle collective

Le type d'attribut c-ou spécifie un nom d'unité organisationnelle pour une collection d'entrées.

(2.5.4.11.1 NAME 'c-ou' SUP ou COLLECTIVE)

3.6 Adresse postale collective

Le type d'attribut c-PostalAddress spécifie une adresse postale pour une collection d'entrées.

(2.5.4.16.1 NAME 'c-PostalAddress' SUP postalAddress COLLECTIVE)

3.7 Code postal collectif

Le type d'attribut c-PostalCode spécifie un code postal pour une collection d'entrées.

(2.5.4.17.1 NAME 'c-PostalCode' SUP postalCode COLLECTIVE)

3.8 Boîte postale collective

Le type d'attribut c-PostOfficeBox spécifie une boîte postale pour une collection d'entrées.

(2.5.4.18.1 NAME 'c-PostOfficeBox' SUP postOfficeBox COLLECTIVE)

3.9 Nom de bureau de livraison physique collectif

Le type d'attribut c-PhysicalDeliveryOfficeName spécifie un nom de bureau physique de livraison pour une collection d'entrées.

(2.5.4.19.1 NAME 'c-PhysicalDeliveryOfficeName' SUP physicalDeliveryOfficeName COLLECTIVE)

3.10 Numéro de téléphone collectif

Le type d'attribut c-TelephoneNumber spécifie un numéro de téléphone pour une collection d'entrées.

(2.5.4.20.1 NAME 'c-TelephoneNumber' SUP telephoneNumber COLLECTIVE)

3.11 Numéro de télex collectif

Le type d'attribut c-TelexNumber spécifie un numéro de télex pour une collection d'entrées.

(2.5.4.21.1 NAME 'c-TelexNumber' SUP telexNumber COLLECTIVE)

3.13 Numéro de télécopie collectif

Le type d'attribut c-FacsimileTelephoneNumber spécifie un numéro de télécopie pour une collection d'entrées.

(2.5.4.23.1 NAME 'c-FacsimileTelephoneNumber' SUP facsimileTelephoneNumber COLLECTIVE)

3.14 Numéro RNIS international collectif

Le type d'attribut c-InternationalISDNNumber spécifie un numéro international RNIS pour une collection d'entrées.

(2.5.4.25.1 NAME 'c-InternationalISDNNumber' SUP internationalISDNNumber COLLECTIVE)

4. Considérations sur la sécurité

Les attributs collectifs, comme les autres attributs, sont soumis à des restrictions de contrôle d'accès et d'autre politique administrative. D'une façon générale, les attributs collectifs accédés via une entrée dans une collection sont gouvernés par des règles qui restreignent l'accès aux attributs de cette entrée. Et l'accès à des attributs collectifs via une sous entrée est gouverné par des règles qui restreignent l'accès aux attributs de cette sous entrée. Cependant, comme LDAP n'a pas de modèle d'accès standard, les particularités de chaque système de contrôle d'accès de serveur peuvent différer.

Les considérations générales de sécurité de LDAP [RFC3377] s'appliquent aussi.

5. Considérations relatives à l'IANA

L'IANA a enregistré les descripteurs LDAP [RFC3383] définis dans cette spécification technique. Le gabarit d'enregistrement suivant est suggéré :

Objet : demande d'enregistrement de descripteur LDAP

Descripteur : voir les commentaires

Identifiant d'objet : voir les commentaires

Adresse de la personne & de messagerie à contacter pour plus d'informations : Kurt Zeilenga <kurt@OpenLDAP.org>

Usage : voir le commentaire

Spécification : RFC3671

Auteur/Contrôleur des changements : IESG

Commentaires :

Nom	Type	OID
c-FacsimileTelephoneNumber	A	2.5.4.23.1
c-InternationalISDNNumber	A	2.5.4.25.1
c-PhysicalDeliveryOffice	A	2.5.4.19.1
c-PostOfficeBox	A	2.5.4.18.1
c-PostalAddress	A	2.5.4.16.1
c-PostalCode	A	2.5.4.17.1
c-TelephoneNumber	A	2.5.4.20.1
c-TelexNumber	A	2.5.4.21.1
c-l	A	2.5.4.7.1
c-o	A	2.5.4.10.1
c-ou	A	2.5.4.11.1
c-st	A	2.5.4.8.1
c-street	A	2.5.4.9.1
collectiveAttributeSubentries	A	2.5.18.12
collectiveAttributeSubentry	O	2.5.17.2
collectiveExclusions	A	2.5.18.7

où le Type A est Attribut et le Type O est ObjectClass.

Les identifiants d'objet utilisés dans le présent document ont été alloués par le sous comité 6 du comité technique conjoint

numéro 1 de l'ISO/CEI pour identifier les éléments du schéma X.500 [X.520]. Le présent document ne fait pas d'allocation d'OID, il donne seulement les descriptions de schéma LDAP avec les éléments existants du schéma X.500.

6. Déclaration de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr>.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

7. Remerciements

Le présent document se fonde sur les Recommandations UIT-T pour l'Annuaire, [X.501], [X.520].

8. Références

8.1 Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (MàJ par [RFC8174](#))
- [RFC2251] M. Wahl, T. Howes et S. Kille, "[Protocole léger d'accès à un répertoire](#) (v3)", décembre 1997.
- [RFC2252] M. Wahl, A. Coulbeck, T. Howes, S. Kille, "[Protocole léger d'accès à un répertoire](#) (v3) : Définitions de syntaxe d'attribut", décembre 1997. (Obsolète, voir [RFC4510](#), [RFC4517](#), [RFC4523](#), [RFC4512](#)) (MàJ par [RFC3377](#)) (P.S.)
- [RFC2255] T. Howes, M. Smith, "[Format d'URL LDAP](#)", décembre 1997. (Obsolète, voir [RFC4510](#), [RFC4516](#)) (P.S.)
- [RFC3377] J. Hodges, R. Morgan, "Protocole léger d'accès à un répertoire (v3) : Spécification technique", septembre 2002. Obsolète, voir [RFC4510](#)) (P.S.)
- [RFC3383] K. Zeilenga, "Autorité d'allocation des numéros de l'Internet (IANA) : Considérations sur le protocole léger d'accès à un répertoire (LDAP)", septembre 2002. (Obsolète, voir [RFC4520](#))
- [RFC3672] K. Zeilenga, "Sous-entrées dans le protocole léger d'accès à un répertoire (LDAP)", décembre 2003. (P.S.)
- [X.501] Recommandation UIT-T X.501, "L'annuaire : Modèles", 1993.

8.2 Références pour information

- [X.500] Recommandation UIT-T X.500, "L'annuaire : aperçu général des concepts, modèles et services", 1993.
- [X.520] Recommandation UIT-T X.520, "L'annuaire : types d'attributs choisis", 1993.

9. Adresse de l'auteur

Kurt D. Zeilenga
OpenLDAP Foundation

mél : Kurt@OpenLDAP.org

10. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2003). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour les besoins du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.