Groupe de travail Réseau
Request for Comments : 3673
Catégorie : Sur la voie de la normalisation

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

Protocole léger d'accès à un répertoire version 3 (LDAPv3) : tous les attributs de fonctionnement

Résumé
Le protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) prend en charge un mécanisme pour demander le retour de tous les attributs d'un utilisateur mais pas tous les attributs de fonctionnement. Le présent document décrit une extension à LDAP que les clients peuvent utiliser pour demande le retour de tous les attributs de fonctionnement.

Table des matières

1. Généralités

La Recommandation UIT-T X.500 [X.500] donne un mécanisme pour que les clients demandent que tous les attributs de fonctionnement soient retournés avec les entrées fournies en réponse à une opération de recherche. Ce mécanisme est souvent utilisé par les clients pour découvrir quels attributs de fonctionnement sont présents dans une entrée.

Le présent documents étend le protocole léger d'accès à un répertoire (LDAP) [RFC3377] à fournir un mécanisme simple que les clients puissent utiliser pour demander le retour de tous les attributs de fonctionnement. Le mécanisme est conçu pour être utilisé avec les clients LDAP d'utilité générale existants (incluant les navigateurs de la Toile qui prennent en charge les URL LDAP) et les API LDAP existantes.

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. Tous les attributs de fonctionnement

La présence de l'attribut de description "+" (ASCII 43) dans la liste des attributs d'une demande de recherche [RFC2251]

DEVRA signifier une demande du retour de tous les attributs de fonctionnement.

Comme avec toutes les demandes de recherche, les mises en œuvre de client devraient noter que le résultat peut ne pas inclure tous les attributs demandés à cause des contrôles d'accès et autres restrictions. Les mises en œuvre de client devraient aussi noter que certains attributs de fonctionnement peuvent n'être retournés que si ils sont demandés par leur nom même quand "+" est présent. C'est parce que certains attributs de fonctionnement sont très coûteux à retourner.

Les serveurs qui prennent en charge cette caractéristique DEVRAIENT publier l'identifiant d'objet 1.3.6.1.4.1.4203.1.5.1 comme valeur de l'attribut 'supportedFeatures' [RFC3674] dans l'entrée spécifique d'un agent système de répertoire (DSE, *DSA Specific Entry*) racine.

3. Considérations d'interopérabilité

Ce mécanisme est spécifiquement conçu pour permettre aux utilisateurs de demander tous les attributs de fonctionnement en utilisant les clients LDAP existants. En particulier, le mécanisme est conçu pour être compatible avec les clients LDAP d'utilité générale existants incluant ceux qui prennent en charge les URL LDAP [RFC2255].

L'ajout de ce mécanisme à LDAP n'est pas estimé devoir causer de problème d'interopérabilité significatif (ceci a été confirmé par des essais). Les serveurs qui ont déjà mis en œuvre la présente spécification DEVRAIENT ignorer le "+" comme une description d'attribut non reconnue selon le paragraphe 4.5.1 de la [RFC2251]. Du point de vue du client, un serveur qui ne retourne pas tous les attributs de fonctionnement quand "+" est demandé devraient être vus comme ayant d'autres 4.5.1 restrictions.

Il est aussi noté que ce mécanisme est estimé n'exiger aucune modification des API LDAP existantes.

4. Considérations sur la sécurité

Le présent document fournit un mécanisme général que les clients peuvent utiliser pour découvrir les attributs. de fonctionnement. Avant l'introduction de ce mécanisme, les attributs de fonctionnement étaient seulement découverts quand ils étaient demandés par leur nom. Certains peuvent avoir vu cela comme une caractéristique de dissimulation. Cependant, cette caractéristique donne un faux sentiment de sécurité car les attributs sont quand même transférables.

Les mises en œuvre DEVRAIENT mettre en place des mécanismes de contrôle d'accès appropriés pour restreindre l'accès aux attributs de fonctionnement.

5. Considérations relatives à l'IANA

Le présent document utilise l'OID 1.3.6.1.4.1.4203.1.5.1 pour identifier la caractéristique décrite ci-dessus. Cet OID a été alloué [ASSIGN] par la Fondation OpenLDAP, sous son allocation d'entreprise privée allouée par l'IANA [PRIVATE], pour l'utiliser dans la présente spécification.

L'enregistrement de cette caractéristique a été réalisé par l'IANA [RFC3674], [RFC3383].

Sujet : Demande d'enregistrement de mécanisme pour le protocole LDAP
Identifiant d'objet : 1.3.6.1.4.1.4203.1.5.1
Description : tous les attributs de fonctionnement
Adresse et messagerie de la personne à contacter pour plus d'informations : Kurt Zeilenga <kurt@openldap.org>
Usage : caractéristique
Spécification : RFC3673
Auteur/Contrôleur des changements : IESG
Commentaires : aucun

6. Remerciements

Le mécanisme "+" a été probablement suggéré pour la première fois par Bruce Greenblatt dans un message de novembre

1998 sur la liste de diffusion du groupe de travail LDAPext de l'IETF.

7. 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 .

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.

[RFC3377] J. Hodges, R. Morgan, "Protocole léger d'accès à un répertoire (v3) : Spécification technique", septembre 2002. (*Obsolète, voir* RFC4510) *(P.S.)*

[RFC3674] K. Zeilenga, "Dispositif de découverte dans le protocole léger d'accès à un répertoire (LDAP)", décembre 2003. (*Obsolète, voir* RFC4512) *(P.S.)*

8.2 Références pour information

[RFC2255] T. Howes, M. Smith, "Format d'URL LDAP", décembre 1997. (*Obsolète, voir* RFC4510, RFC4516) *(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)

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

[ASSIGN] OpenLDAP Foundation, "OpenLDAP OID Delegations", http://www.openldap.org/foundation/oid-delegate.txt

[PRIVATE] IANA, "Private Enterprise Numbers", http://www.iana.org/assignments/enterprise-numbers

9. Adresse de l'auteur

Kurt D. Zeilenga
OpenLDAP Foundation
mél : Kurt@OpenLDAP.org

10. Déclaration complète de droits de reproduction

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