Groupe de travail Réseau
Request for Comments : 4370
Catégorie : Sur la voie de la normalisation

R. Weltman, Yahoo!, Inc.
février 2006
Traduction Claude Brière de L'Isle

Contrôle d'autorisation par mandataire du protocole léger d'accès à un répertoire (LDAP)

Résumé
Le présent document définit le contrôle d'autorisation par mandataire du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*). Le contrôle d'autorisation par mandataire permet à un client de demander qu'une opération soit traitée sous une identité d'autorisation fournie au lieu de sous l'identité d'autorisation courante associée à la connexion.

1. Introduction

L'autorisation par mandataire permet à un client de demander qu'une opération soit traitée sous une identité d'autorisation fournie au lieu de l'identité d'autorisation courante associée à la connexion. Le présent document définit la prise en charge de l'autorisation par mandataire en utilisant le mécanisme Control [RFC2251]. Le protocole léger d'accès à un répertoire [RFC3377] prend en charge l'utilisation de l'authentification simple et couche de sécurité [RFC2222] pour l'authentification et pour fournir une identité d'autorisation distincte de l'identité d'authentification, où l'identité d'autorisation s'applique à toute la session LDAP. Le contrôle d'autorisation par mandataire donne un mécanisme pour spécifier une identité d'autorisation sur la base de l'opération, au bénéfice des clients qui ont besoin d'effectuer des opérations de façon efficace au nom de plusieurs utilisateurs.

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

2. Publication de la prise en charge du contrôle d'autorisation de mandataire

La prise en charge du contrôle d'autorisation par mandataire est indiquée par la présence de l'identifiant d'objet (OID) "2.16.840.1.113730.3.4.18" dans l'attribut supportedControl [RFC2252] de l'entrée spécifique de DSA (DSE, *DSA-specific Entry*) racine d'un serveur.

3. Contrôle d'autorisation par mandataire

Un seul contrôle d'autorisation par mandataire peut être inclus dans tout message search, compare, modify, add, delete, ou modification de nom distinctif (DN, *Distinguished Name*) ou demande d'opération étendue. L'exception est toute extension qui cause un changement dans l'authentification, l'autorisation, ou la confidentialité des données [RFC2829], comme un Start TLS [RFC2830] au titre du champ Controls du message LDAP, comme défini dans la [RFC2251].

Le type de contrôle du contrôle d'autorisation par mandataire est "2.16.840.1.113730.3.4.18".

La criticité DOIT être présente et DOIT être VRAI. Cette exigence protège les clients contre la soumission d'une demande qui serait exécutée avec une identité d'autorisation non prévue.

Les clients DOIVENT inclure le fanion criticité et DOIVENT le régler à VRAI. Les serveurs DOIVENT rejeter toute demande contenant un contrôle d'autorisation par mandataire, sans un fanion criticité ou avec ce fanion réglé à FAUX, avec une erreur protocolError. Ces exigences protègent les clients contre la soumission d'une demande qui serait exécutée avec une identité d'autorisation non prévue.

La valeur de controlValue DEVRA être présente et DEVRA soit contenir un identifiant authzId [RFC2829] représentant l'identité d'autorisation pour la demande, soit être vide si une association anonyme doit être utilisée.

Le mécanisme pour déterminier les droits d'accès de mandataire est spécifique de la politique d'autorisation de mandataire du serveur.

Si l'identité d'autorisation demandée est reconnue par le serveur, et si le client est autorisé à adopter l'identité d'autorisation demandée, la demande va être exécutée comme si elle était soumise par l'identité d'autorisation par mandataire ; sinon, le code de résultat 123 est retourné.

4. Considérations de mise en œuvre

Une interaction possible de contrôle d'autorisation par mandataire et d'accès normal est illustrée ici. Durant l'évaluation d'une demande de recherche, une entrée qui aurait été retournée de la recherche (si elle avait été soumise directement par l'identité d'autorisation par mandataire) peut n'être pas retournée si le serveur trouve que le demandeur n'a pas le droit d'assumer l'identité demandée pour rechercher l'entrée, même si l'entrée est dans la portée d'une demande de recherche sous un DN de base qui implique bien de tels droits. Cela signifie que moins de résultats, ou pas de résultat du tout, peuvent être retournés qu'il n'en aurait été si l'identité d'autorisation par mandataire avait produit directement la demande. Un exemple d'un tel cas peut être un système avec un contrôle d'accès de granularité fine, où le demandeur du droit de mandataire a les droits de mandataire au sommet de l'arborescence de recherche, mais pas à un point ou en dessous de ce ou ces points au sein de l'arborescence.

5. Considérations sur la sécurité

La méthode de contrôle d'autorisation par mandataire est soumise aux considérations générales de sécurité de LDAP [RFC2251] [RFC2829] [RFC2830]. Le contrôle peut être passé sur un canal sûr aussi bien que non sûr.

Le contrôle permet de passer une identité d'autorisation supplémentaire. Dans certains déploiements, ces identités peuvent contenir des informations confidentielles qui exigent une protection.

Noter que le serveur est chargé de déterminer si une demande d'autorisation par mandataire doit être honorée. Les utilisateurs "anonymes" NE DEVRAIENT PAS être admis à assumer l'identité d'autres.

6. Considérations relatives à l'IANA

L'OID "2.16.840.1.113730.3.4.18" est réservé pour le contrôle d'autorisation par mandataire. Il a été enregistré comme mécanisme du protocole LDAP [RFC3383].

Un code de résultat (123) a été alloué par l'IANA pour le cas où le serveur n'exécute pas une demande utilisant l'identité d'autorisation par mandataire.

7. Remerciements

Mark Smith, anciennement de Netscape Communications Corp., Mark Wahl, anciennement de Sun Microsystems, Inc., Kurt Zeilenga de OpenLDAP Foundation, Jim Sermersheim de Novell, et Steven Legg de Adacel ont contribué à ce document par leur relecture.

8. 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)

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

[RFC2251] M. Wahl, T. Howes et S. Kille, "Protocole léger d'accès à un répertoire (v3)", décembre 1997. (*Obsolète, voir* RFC4511)

[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, RFC4512, RFC4517, RFC4523) *(P.S.)*

[RFC2829] M. Wahl et autres, "Méthodes d'authentification pour LDAP", mai 2000. (*Obsolète, voir* RFC4513, RFC4510) *(P.S.)*

[RFC2830] J. Hodges, R. Morgan, M. Wahl, "Protocole léger d'accès à un répertoire (v3) : extension pour la sécurité de la couche transport", mai 2000. (*Obsolète, voir* RFC4511, RFC4513, RFC4510) *(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)

Adresse de l'auteur

Rob Weltman
Yahoo!, Inc.
701 First Avenue
Sunnyvale, CA 94089
USA

téléphone : +1 408 349-5504
mél : robw@worldspot.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.