Groupe de travail Réseau
Request for Comments : 4530
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

K. Zeilenga
OpenLDAP Foundation

juin 2006
août 2007

Protocole léger d'accès à un répertoire (LDAP) ; opération "Who am I?"

Résumé
La présente spécification fournit un mécanisme permettant aux clients du protocole léger d'accès aux répertoires (LDAP, *Lightweight Directory Access Protocol*) d'obtenir l'identité d'autorisation que le serveur a associée à l'utilisateur ou à l'entité d'application. Ce mécanisme est spécifié comme opération d'extension de LDAP appelée opération LDAP "Who am I?".

1 Fondements et destination

La présente spécification décrit une opération du protocole léger d'accès aux répertoires (LDAP) [RFC4510] que les clients peuvent utiliser pour obtenir l'identité d'autorisation principale, dans sa forme principale, que le serveur avait associé à l'utilisateur ou à l'entité d'application. L'opération est appelée "Who am I?"

La présente spécification est destinée à remplacer le mécanisme existant de commande d'identité d'autorisation de la [RFC3829], qui utilise les commandes de demande et réponse Bind pour demander et retourner l'identité d'autorisation. Les commandes Bind ne sont pas protégées par les couches de sécurité établies par l'opération Bind qui les inclut. Alors qu'il est possible d'établir des couches de sécurité en utilisant StartTLS [RFC4511][RFC4513] avant l'opération Bind, il est souvent souhaitable d'utiliser des couches de sécurité établies par l'opération Bind. Une opération étendue envoyée après une opération Bind est protégée par les couches de sécurité établies par l'opération Bind.

Il y a d'autres cas où il est souhaitable de demander l'identité d'autorisation que le serveur avait associé au client indépendamment de l'opération Bind. Par exemple, l'opération "Who am I?" peut être enrichie d'une commande d'autorisation mandatée de la [RFC4370] pour déterminer l'identité d'autorisation que le serveur associe à l'identité affirmée dans la commande d'autorisation mandatée. L'opération "Who am I?" peut aussi être utilisée avant l'opération Bind.

Les serveurs associent souvent plusieurs identités d'autorisation au client, et chaque identité d'autorisation peut être représentée par plusieurs chaînes authzId [RFC4513]. Cette opération demande et retourne la authzId que le serveur considère comme principale. Dans la présente spécification, les termes "identité d'autorisation" et "authzId" doivent généralement être compris respectivement comme "identité d'autorisation principale" et "authzId principal".

1.1 Conventions utilisées dans le présent document

Dans le présent document, les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14 [RFC2119].

2 L’opération "Who am I?"

L’opération "Who am I?" est définie comme une opération étendue de LDAP [RFC4511] identifiée par l’identifiant d’objet (OID) whoamiOID. Cette section précise la syntaxe des messages de demande et de réponse whoami de l’opération.

whoamiOID ::= "1.3.6.1.4.1.4203.1.11.3"

2.1 La demande whoami

La demande whoami est une ExtendedRequest avec un champ requestName qui contient l’OID whoamiOID et un champ requestValue absent. Par exemple, une demande whoami pourrait être codée comme la séquence d’octets (en hexadécimal) suivante :
30 1e 02 01 02 77 19 80 17 31 2e 33 2e 36 2e 31 2e 34 2e 31 2e 34 32 30 33 2e 31 2e 31 31 2e 33

2.2 La réponse whoami

La réponse whoami est une ExtendedResponse où le champ responseName est absent et le champ de réponse, s’il est présent, est vide ou est un authzId [RFC4513]. Par exemple, une réponse whoami retournant le authzId "u:xxyyz@EXAMPLE.NET" (en réponse à l’exemple de demande) serait codé comme la séquence d’octets (en hexadécimal) suivante :

30 21 02 01 02 78 1c 0a 01 00 04 00 04 00 8b 13 75 3a 78 78 79 79 7a 40 45 58 41 4d 50 4c 45 2e 4e 45 54

3 Sémantique opérationnelle

L’opération "Who am I?" fournit un mécanisme, une demande whoami, permettant au client de demander que le serveur retourne l’identité d’autorisation qu’il associe actuellement au client. Elle fournit aussi un mécanisme, une réponse whoami, pour que le serveur réponde à cette demande.

Les serveurs indiquent leur prise en charge de cette opération étendue en fournissant un identifiant d’objet whoamiOID comme valeur du type d’attribut 'supportedExtension' dans leur DSE racine. Le serveur ne DEVRAIT publier cette extension que lorsque le client veut et est capable d’effectuer cette opération.

Si le serveur veut et est capable de fournir l’identité d’autorisation qu’il associe à ce client, le serveur DEVRA retourner une réponse whoami avec un resultCode de succès. Si le serveur traite le client comme une entité anonyme, le champ de réponse sera présent mais vide. Autrement, le serveur fournira le authzId [RFC4513] représentant l’identité d’autorisation qu’il associe actuellement au client dans le champ de réponse.

Si le serveur ne veut pas ou est incapable de fournir l’identité d’autorisation qu’il associe au client, le serveur DEVRA retourner une réponse whoami avec un resultCode d’échec approprié (tel que operationsError, protocolError, confidentialityRequired, insufficientAccessRights, busy, unavailable, unwillingToPerform, ou autre) et un champ de réponse absent.

Comme décrit dans la [RFC4511] et la [RFC4513], une session LDAP a une association "anonyme" jusqu’à ce que le client ait été authentifié avec succès en utilisant l’opération Bind. Les clients NE DOIVENT PAS invoquer l’opération "Who am I?" alors qu’une opération Bind est en cours, y compris entre deux demandes Bind requests faites au titre d’une opération Bind multi étapes. Lorsqu’une demande whoami est reçue en violation de cette interdiction absolue, le serveur devrait retourner une réponse whoami avec un resultCode de operationsError.

4 Extension de l’opération "Who am I?" avec des commandes

Des spécifications futures pourront étendre l’opération "Who am I?" en utilisant le mécanisme de commande de la [RFC4511]. Lorsqu’elle est étendue par des commandes, l’opération "Who am I?" demande et retourne l’identité d’autorisation que le serveur associe au client dans un contexte particulier indiqué par les commandes.

4.1 Commande d'autorisation mandatée

La commande d'autorisation mandatée de la [RFC4370] est utilisée par les clients pour demander que le fonctionnement de l'opération à laquelle elle est rattachée soit subordonné à l'autorisation d'une identité supposée. Le client fournit l'identité qui sera supposée dans la commande de demande d'autorisation mandatée. Si le client est autorisé à supposer l'identité demandée, le serveur exécutera l'opération comme si l'identité demandée avait produit l'opération.

Comme les serveurs transposent souvent la authzId affirmée en une autre identité [RFC4513], il est souhaitable de demander que le serveur fournisse le authzId qu'il associe à l'identité supposée.

Lorsqu'une commande d'autorisation mandatée est rattachée à l'opération "Who am I?", l'opération demande le retour de la the authzId que le serveur associe à l'identité affirmée dans la commande d'autorisation mandatée. Le code de résultat authorizationDenied (123) est utilisé pour indiquer que le serveur ne permet pas au client de supposer l'identité affirmée.

5 Considérations sur la sécurité

Les identités associées aux utilisateurs peuvent être des informations sensibles. Lorsqu'elles le sont, les couches de sécurité [RFC4511][RFC4513] devraient être établies pour protéger ces informations. Ce mécanisme est spécifiquement conçu pour permettre aux couches de sécurité établies par une opération Bind de protéger l'intégrité et/ou la confidentialité de l'identité d'autorisation.

Les serveurs peuvent placer un contrôle d'accès ou d'autres restrictions à l'utilisation de cette opération. Comme indiqué à la Section 3, le serveur DEVRAIT publier cette extension lorsqu'il veut effecteur cette opération et en est capable. Comme avec toutes les autres opérations d'extension, les considérations générales sur la sécurité de LDAP [RFC4510] s'appliquent.

6 Considérations relatives à l'IANA

L'OID 1.3.6.1.4.1.4203.1.11.3 sert à identifier l'opération étendue "Who am I?" de LDAP. Cet OID a été alloué [ASSIGN] par la fondation OpenLDAP, dans son allocation d'entreprise privée [PRIVATE] allouée par l'IANA, pour être utilisé dans la présente spécification.

L'enregistrement de ce mécanisme de protocole [RFC4520] a été effectué par l'IANA.

Sujet : Demande d'enregistrement de mécanisme de protocole pour LDAP
Identifiant d'objet : 1.3.6.1.4.1.4203.1.11.3
Description : Who am I?
Personne et adresse de messagterie à contacter pour des précisions :
Kurt Zeilenga kurt@openldap.org
Usage : Opération d'extension
Spécification : RFC 4532
Auteur/Contrôleur des modifications : IESG
Commentaire : aucun

7 Remerciements

Ce document fait des emprunts à des travaux antérieurs dans ce domaine, en particulier à "Commande de réponse d'authentification" [RFC3829] de Rob Weltman, Mark Smith, et Mark Wahl.

L'opération LDAP "Who am I?" tire son nom de la commande UNIX whoami(1). La commande whoami(1) affiche l'identifiant effectif de l'utilisateur.

8 Références

8.1 Références normatives

[RFC2119] Bradner, S., "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[RFC4370] Weltman, R., "Protocole léger d'accès aux répertoires (LDAP) Commande d'autorisation mandatée", RFC 4370, février 2006.

[RFC4510] Zeilenga, K., éd, "Protocole léger d'accès aux répertoires (LDAP) : plan d'accès des spécifications techniques, RFC 4510, juin 2006.

[RFC4511] Sermersheim, J., éd., "Protocole léger d'accès aux répertoires (LDAP) : le protocole", RFC 4511, juin 2006.

[RFC4513] Harrison, R., Ed., "Protocole léger d'accès aux répertoires (LDAP) : Méthodes d'authentification et mécanismes de sécurité", RFC 4513, juin 2006.

8.2 Références informatives

[RFC3829] Weltman, R., Smith, M., et M. Wahl, "Protocole léger d'accès aux répertoires (LDAP) : Commandes de demande et de réponse d'identité d'autorisation", RFC 3829, juillet 2004.

[RFC4520] Zeilenga, K., "Autorité d'allocation des numéros de l'Internet (IANA) Considérations sur le protocole léger d'accès aux répertoires (LDAP)", BCP 64, RFC 4520, juin 2006.

[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.

Adresse de l'auteur
Kurt D. Zeilenga
OpenLDAP Foundation
mél : Kurt@OpenLDAP.org

Remerciement
Le financement de la fonction d'édition des RFC est fourni par la Administrative Support Activity (IASA) de l'IETF.