Groupe de travail Réseau	K. Zeilenga
Request for Comments : 4528	OpenLDAP Foundation
Catégorie : En cours de normalisation	juin 2006
Traduction Claude Brière de L'Isle	01/08/07

Protocole léger d'accès à un répertoire (LDAP) ; commande d'assertion

Résumé

Le présent document définit la commande d'assertion du protocole léger d'accès aux répertoires LDAP, *Lightweight Directory Access Protocol*), qui permet à un client de spécifier qu'une opération de répertoire ne devrait être traitée que si une assertion appliquée à l'entrée cible de l'opération est vraie. Elle peut être utilisée pour construire "essai et établissement", "essai et élimination", et autres opérations conditionnelles.

1 Généralités

Le présent document définit la commande d'assertion du protocole léger d'accès aux répertoires LDAP [RFC4510]. La commande d'assertion permet au client de spécifier une condition qui doit être vraie pour que l'opération soit traitée normalement. Autrement, l'opération n'est pas effectuée. Par exemple, la commande peut être utilisée avec l'opération Modify [RFC4511] pour effectuer les opérations élémentaires "essai et établissement", "essai et élimination".

La commande peut être rattachée à toute opération de mise à jour pour prendre en charge ajout, suppression, modification, et renommage conditionnels de l'objet cible. La condition affirmée est évaluée comme partie intégrante de l'opération.

La commande peut aussi être utilisée avec l'opération de recherche *(search)*. Ici, l'assertion s'applique à l'objet de base de la recherche avant de chercher les objets qui correspondent à l'objet et filtre de la recherche.

La commande peut aussi être utilisée avec l'opération compare. Ici, elle étend l'opération compare pour permettre une assertion complexe.

2 Terminologie

Les éléments de protocole sont décrits en utilisant l'ASN.1 [X.680] avec étiquettes implicites. Le terme "codé en BER" signifie que l'élément est à coder en utilisant les règles de codage de base *(Basic Encoding Rules)* [X.690] avec les restrictions précisées au paragraphe 5.1 de la [RFC4511].

DSA signifie agent (ou serveur) de système de répertoire *(Directory System Agent)*.
DSE signifie entrée spécifique de DSA *(DSA-specific Entry)*.

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].

3 Commande d'assertion

La commande d'assertion est une commande LDAP [RFC4511] dont le controlType est 1.3.6.1.1.12 et dont la controlValue est un filtre codé en BER [Protocole, paragraphe 4.5.1]. La criticité peut être TRUE *(vrai)* ou FALSE *(faux)*. Il n'y a pas de commande de réponse correspondante.

La commande est appropriée aussi bien pour les opérations d'interrogation que de mise à jour de LDAP [RFC4511], y compris Add *(ajouter)*, Compare *(comparer)*, Delete *(supprimer)*, Modify *(modifier)*, ModifyDN *(renommer)*, et Search *(rechercher)*. Elle n'est pas appropriée pour les opérations Abandon *(abandonner)*, Bind *(lier)*, Unbind *(délier)*, et StartTLS *(lancement de la sécurité de couche Transport)*.

Lorsque la commande est rattachée à une demande LDAP, le traitement de la demande est conditionné à l'évaluation du filtre appliqué à la cible de l'opération. Si le filtre évalue à VRAI, la demande est alors traitée normalement. Si le filtre évalue à FAUX ou à Indéfini, le resultCode *(code de résultat)* assertionFailed *(échec de l'assertion)* (122) est retourné, et aucun autre traitement n'est effectué.

Pour les opérations Add, Compare, et ModifyDN, la cible est indiquée par le champ d'entrée dans la demande. Pour les opérations Modify, la cible est indiquée par le champ d'objet. Pour les opérations Delete, la cible est indiquée par le type DelRequest. Pour les opérations Compare et toutes les opérations de mise à jour, l'évaluation de l'assertion DOIT être effectuée comme partie intégrante de l'opération. C'est-à-dire que l'évaluation de l'assertion et le traitement normal de l'opération DEVRAONT être effectuées comme une action élémentaire.

Pour les opérations Search, la cible est indiquée par le champ baseObject, et l'évaluation est faite après avoir "trouvé" mais avant "searching" [RFC4511]. Et donc, aucune référence d'entrées ou de continuations n'est retournée si l'assertion échoue.

Les serveurs qui mettent en oeuvre la présente spécification technique DEVRAIENT publier l'identifiant d'objet 1.3.6.1.1.12 comme valeur de l'attribut 'supportedControl' [RFC4512] dans leur DSE racine. Un serveur PEUT choisir de ne publier cette extension que lorsque le client est autorisé à l'utiliser.

D'autres documents peuvent spécifier comment cette commande s'applique aux autres opérations LDAP. En le faisant, ils doivent déclarer comment est déterminée l'entrée cible.

4 Considérations pour la sécurité

Le filtre peut, comme d'autres composants de la demande, contenir des informations sensibles. Lorsque c'est le cas, ces informations devraient être protégées de façon appropriée.

Comme avec tout mécanisme général d'assertion, le mécanisme peut être utilisé pour déterminer le contenu d'un répertoire. Et donc, ce mécanisme DEVRAIT être soumis aux contrôles d'accès appropriés.

Certaines assertions peuvent être très complexes, exigeant un temps et des ressources significatives pour les évaluer. ET donc, ce mécanisme DEVRAIT être soumis aux contrôles administratifs appropriés.

Les considérations sur la sécurité pour les opérations de base [RFC4511] étendues par cette commande, ainsi que les considérations sur la sécurité générales de LDAP [RFC4510], s'appliquent de façon générale à la mise en oeuvre et l'utilisation de cette extension.

5 Considérations relatives à l'IANA

5.1 Identifiant d'objet

L'IANA a alloué un identifiant d'objet LDAP [RFC4520] pour identifier la commande d'assertion LDAP définie dans le présent document.

Sujet : Demande d'enregistrement d'identifiant d'objet LDAP
Personne et adresse de messagerie à contacter pour des précisions :

Kurt Zeilenga <kurt@OpenLDAP.org>
Spécification : RFC 4528
Auteur/Contrôleur des modifications : IESG
Commentaires : Identifie la commande d'assertion de LDAP

5.2 Mécanisme de protocole LDAP

L'enregistrement de ce mécanisme de protocole [RFC4520] est demandé.

Sujet : Demande d'enregistrement de mécanisme de protocole LDAP
Identifiant d'objet : 1.3.6.1.1.12
Description : Commande d'assertion
Personne et adresse de messagerie à contacter pour des précisions :
Kurt Zeilenga <kurt@openldap.org>
Usage : Commande
Spécification : RFC 4528
Auteur/Contrôleur des modifications : IESG
Commentaires : aucun

5.3 Code de résultat LDAP

L'IANA a alloué un code de résultat LDAP [RFC4520] appelé 'assertionFailed' (122).

Sujet : Enregistrement de code de résultat LDAP
Personne et adresse de messagerie à contacter pour des précisions :
Kurt Zeilenga <kurt@OpenLDAP.org>
Nom de code de résultat : assertionFailed
Spécification : RFC 4528
Auteur/Contrôleur des modifications : IESG
Commentaire : aucun

6 Remerciements

Le concept de commande d'assertion LDAP est attribué à Morteza Ansari.

7 Références

7.1 Références normatives

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

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

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

[RFC4512] Zeilenga, K., "Protocole léger d'accès aux répertoires (LDAP) : modèles d'informations de répertoires", RFC 4512, juin 2006.

[X.680] Union Internationale des Télécommunications - Secteur de la Normalisation des Télécommunications, "Notation numéro un de syntaxe abstraite (ASN.1) - Spécification de la notation de base", X.680 (1997) (aussi ISO/CEI 8824-1:1998).

[X.690] Union Internationale des Télécommunications - Secteur de la Normalisation des Télécommunications, "Spécification des règles de codage ASN.1 : Règles de codage de base (BER), Règles de codage canonique (CER), et Règles de codage distinctives (DER)", X.690 (1997) (aussi ISO/CEI 8825-1:1998).

7.2 Références informatives

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

Adresse de l'auteur

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

Déclaration de copyright

Propriété intellectuelle

Remerciement

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