Groupe de travail Réseau
Request for Comments : 4526
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) ; commandes d'entrée de lecture

Résumé

Le présent document spécifie une extension au protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) pour permettre au client de lire l'entrée cible d'une opération de mise à jour. Le client peut demander à lire l'entrée avant et/ou après que les modifications s'appliquent. Ces lectures sont fait comme une partie élémentaire de l'opération de mise à jour.

1 Fondements et destination

Le présent document spécifie une extension du protocole léger d'accès à un répertoire (LDAP) [RFC4510] pour permettre au client de lire l'entrée cible d'une opération de mise à jour (par exemple, Add, Delete, Modify, ModifyDN). L'extension utilise des commandes [RFC4511] attachées aux demandes pour réclamer et retourner des copies de l'entrée cible. Une commande de demande, appelée commande de demande Pre-Read *(pré lecture)*, indique qu'une copie de l'entrée est à retourner avant l'application de la mise à jour. Une autre commande, appelée commande de demande Post-Read *(après lecture)*, indique qu'une copie de l'entrée est à retourner après l'application de la mise à jour. Chaque commande de demande a une commande de réponse correspondante utilisée pour retourner l'entrée.

Pour garantir une isolation appropriée, les commandes sont traitées comme une partie élémentaire de l'opération de mise à jour.

La fonctionnalité offerte par ces commandes est fondée sur la fonctionnalité similaire du protocole d'accès à l'annuaire X.500 (DAP, *Directory Access Protocol*) [X.511].

Les commandes Pre-Read peuvent être utilisées pour obtenir des valeurs remplacées ou supprimées d'attributs modifiés ou une copie de l'entrée supprimée.

Les commandes Post-Read peuvent être utilisées pour obtenir les valeurs d'attributs opérationnels, tels que les attributs 'entryUUID' [RFC4530] et 'modifyTimestamp' [RFC4512], mis à jour par le serveur au titre de l'opération de mise à jour.

2 Terminologie

Les éléments du protocole sont décrits en utilisant l'ASN.1 [X.680] avec des étiquettes implicites. Le terme "BER-encoded" signifie que l'élément est à coder en utilisant les règles de codage de base [X.690] avec les restrictions précisées au paragraphe 5.1 de la [RFC4511].

DN signifie Distinguished Name *(nom distinctif)*.
DSA signifie Directory System Agent *(agent de système de répertoire)* (c'est-à-dire, un serveur de répertoire).

DSE signifie DSA-specific Entry *(entrée spécifique de DSA)*.

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 Commandes Read Entry

3.1 Commandes de pré lecture *(Pre-Read)*

Les commandes de demande et de réponse de pré lecture sont identifiées par l'identifiant d'objet 1.3.6.1.1.13.1. Les serveurs qui mettent en oeuvre ces commandes DEVRAIENT publier 1.3.6.1.1.13.1 comme valeur du 'supportedControl' [RFC4512] dans leur DSE racine.

La commande de demande de pré lecture est une commande LDAP [RFC4511] dont le controlType est 1.3.6.1.1.13.1 et dont la controlValue est une AttributeSelection [RFC4511] codée en BER, telle qu'étendue par la [RFC3673]. La criticité peut être TRUE ou FALSE. Cette commande est appropriée pour les messages LDAP modifyRequest, delRequest, et modDNRequest.

La commande de réponse correspondant est une commande LDAP dont le controlType est 1.3.6.1.1.13.1 et dont la controlValue, une CHAINE D'OCTETS, contient une SearchResultEntry codée en BER. La criticité peut être TRUE ou FALSE. Cette commande est appropriée pour les messages LDAP modifyResponse, delResponse, et modDNResponse avec un resultCode de succès (0).

Lorsque la commande de demande est rattachée à une demande LDAP appropriée de mise à jour, la commande demande le retour d'une copie de l'entrée cible avant l'application de la mise à jour. AttributeSelection indique, comme exposé dans la [RFC4511][RFC3673], quels attributs devraient apparaître dans la copie. Le serveur va retourner une SearchResultEntry contenant, sous réserve des contrôles d'accès et autres contraintes, les valeurs des attributs demandés.

Le traitement normal de l'opération de mise à jour et le traitement de cette commande DOIVENT être effectués comme une action élémentaire isolée des autres opérations de mise à jour.

Si l'opération de mise à jour échoue (dans le traitement normal ou de contrôle), aucune commande de réponse de pré lecture n'est fournie.

3.2 Commandes après lecture

Les commandes de demande et réponse Post-Read sont identifiées par l'identifiant d'objet 1.3.6.1.1.13.2. Les serveurs qui mettent en oeuvre ces commandes DEVRAIENT publier 1.3.6.1.1.13.2 comme valeur de 'supportedControl' [RFC4512] dans leur DSE racine.

La commande de demande Post-Read est une commande LDAP [RFC4511] dont le controlType est 1.3.6.1.1.13.2 et dont la controlValue, une CHAINE D'OCTETS, contient un AttributeSelection [RFC4511] codé en BER, tel qu'étendu par la [RFC3673]. La criticité peut être TRUE ou FALSE. Cette commande est appropriée pour les messages LDAP addRequest, modifyRequest, et modDNRequest.

La commande de réponse correspondante est une commande LDAP dont le controlType est 1.3.6.1.1.13.2 et dont la controlValue est une SearchResultEntry codée en BER. La criticité peut être TRUE ou FALSE. Cette commande est appropriée pour les messages LDAP addResponse, modifyResponse, et modDNResponse avec un resultCode de succès (0).

Lorsque la commande de demande est rattachée à une demande LDAP de mise à jour appropriée, la commande demande le retour d'une copie de l'entrée cible après l'application de la mise à jour. AttributeSelection indique, comme exposé dans la [RFC4511][RFC3673], quels attributs doivent apparaître dans la copie. Le serveur doit retourner un SearchResultEntry contenant, sous réserve des contrôles d'accès et autres contraintes, les valeurs des attributs demandés.

Le traitement normal de l'opération de mise à jour et le traitement de cette commande DOIVENT être effectués comme

une action élémentaire, isolée des autres opérations de mise à jour.

Si l'opération de mise à jour échoue (dans le traitement normal ou de contrôle), aucune commande de réponse Post-Read n'est fournie.

4 Interaction avec les autres commandes

Les commandes Pre-Read et Post-Read peuvent être combinées avec chacune des autres et/ou avec divers autres commandes. Lorsqu'elle est combinée avec la commande d'assertion [RFC4528] et/ou la commande manageDsaIT [RFC3296], la sémantique de chaque commande incluse dans la combinaison s'applique. Les commandes Pre-Read et Post-Read peuvent être combinées avec d'autres commandes selon ce qui est précisé dans les autres spécifications techniques.

5 Considérations pour la sécurité

Les commandes définies dans le présent document étendent les opérations de mise à jour de façon à prendre en charge les capacités de lecture. Les serveurs DOIVENT s'assurer que le client est autorisé à lire les informations fournies dans cette commande et que le client est autorisé à effectuer la mise à jour de répertoire demandée.

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

6 Considérations relatives à l'IANA

L'enregistrement des valeurs de protocole suivantes [RFC4520] a été réalisé par l'IANA.

6.1 Identifiant d'objet

L'IANA a enregistré un Identifiant d'objet LDAP pour identifier les éléments de protocole LDAP définis dans la présent document.

Sujet : Demande d'enregistrement d'identifiant d'objet LDAP
Adresse personnelle et de messagerie à contacter pour des précisions :
Kurt Zeilenga <kurt@OpenLDAP.org>
Spécification : RFC 4527
Auteur/Contrôleur des modifications: IESG
Commentaire : Identifie les commandes LDAP d'entrée de lecture

6.2 Mécanismes de protocole LDAP

L'IANA a enregistré le mécanisme de protocole LDAP décrit dans la présent document.

Sujet : Demande d'enregistrement de mécanisme du protocole LDAP
Identifiant d'objet : 1.3.6.1.1.13.1
Description : Commande Pre-read LDAP
Adresse personnelle et de messagerie à contacter pour des précisions :
Kurt Zeilenga <kurt@openldap.org>
Usage : Commande
Spécification : RFC 4527
Auteur/Contrôleur des modifications: IESG
Commentaires : aucun

Sujet : Demande d'enregistrement de mécanisme du protocole LDAP
Identifiant d'objet : 1.3.6.1.1.13.2
Description: LDAP Post-read Control

Adresse personnelle et de messagerie à contacter pour des précisions :
Kurt Zeilenga <kurt@openldap.org>
Usage : Commande
Specification: RFC 4527
Auteur/Contrôleur des modifications: IESG
Commentaires : aucun

7 Remerciements

Les commandes LDAP Pre-Read et Post-Read sont modélisées d'après des capacités similaires offertes dans le protocole DAP [X.511].

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.

[RFC3296] Zeilenga, K., "Named Subordinate References in Lightweight Directory Access Protocol (LDAP) Directories", RFC 3296, July 2002.

[RFC3673] Zeilenga, K., "Protocole léger d'accès aux répertoires version 3 (LDAPv3): Attributs opérationnels", RFC 3673, décembre 2003.

[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.

[RFC4528] Zeilenga, K., "Protocole léger d'accès aux répertoires (LDAP) : commande d'assertion", RFC 4528, 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).

8.2 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.

[RFC4530] Zeilenga, K., "Protocole léger d'accès aux répertoires (LDAP) Attribut opérationnel EntryUUID", RFC 4530, juin 2006.

[X.511] Union Internationale des Télécommunications - Secteur de la Normalisation des Télécommunications, "L'Annuaire : Définition de service abstraite", X.511 (1993) (aussi ISO/IEC 9594-3:1993).

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.