Groupe de travail Réseau
Request for Comments : 3909
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

K. Zeilenga, OpenLDAP Foundation

octobre 2004

Opération Cancel du protocole léger d'accès à un répertoire (LDAP)

Résumé
La présente spécification décrit une opération d'extension du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) pour annuler (ou abandonner) une opération en cours. À la différence de l'opération Abandon de LDAP, mais comme l'opération Abandon du protocole d'accès de répertoire X.511 (DAP, *Directory Access Protocol*) cette opération a une réponse qui donne une indication de son résultat.

1. Fondements et destination

Le protocole léger d'accès à un répertoire (LDAP) [RFC3377] prévoit une opération Abandon [RFC2251] que les clients peuvent utiliser pour annuler d'autres opérations. L'opération Abandon n'a pas de réponse et n'exige pas de réponse de la part de l'opération abandonnée. Cette sémantique n'apporte au client aucune indication claire sur le résultat de l'opération Abandon.

Le protocole d'accès de répertoire X.511 [X.511] prévoit une opération Abandon qui a une réponse et exige aussi que l'opération abandonnée retourne une réponse indiquant qu'elle a été annulée. L'opération Cancel de LDAP est modélisée d'après l'opération Abandon de DAP.

L'opération Cancel de LDAP DEVRAIT être utilisée à la place de l'opération Abandon de LDAP lorsque le client a besoin d'une indication du résultat. Cette opération peut être utilisée pour annuler des opérations d'interrogation aussi bien que de mise à jour.

Les éléments de protocole sont décrits en utilisant l'ASN.1 [X.680] avec des étiquettes implicites. Le terme "codé en BER" signifie que l'élément est à coder en utilisant les règles de codage de base (BER, *Basic Encoding Rules*) [X.690] avec les restrictions précisées au paragraphe 5.1 de la [RFC2251].

On utilise l'acronyme DSA *(Directory System Agent)* pour un agent (ou serveur) de système de répertoire et celui de DSE *(DSA-specific Entry)* pour une entrée spécifique de DSA.

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 les BCP 14, [RFC2119].

2. Opération Cancel

L'opération Cancel est définie comme une opération d'extension de LDAP telle que définie au paragraphe 4.12 de la [RFC2251] avec l'identifiant d'objet 1.3.6.1.1.8. Cette section détaille la syntaxe des messages de demande et de réponse Cancel et définit les codes de résultat LDAP supplémentaires.

2.1 Demande Cancel

La demande Cancel est une demande étendue (ExtendedRequest) dont le champ Nom de demande (requestName) contient 1.3.6.1.1.8 et un champ Valeur de demande (requestValue) qui contient une valeur de cancelRequestValue codée en BER.

```
cancelRequestValue ::= SEQUENCE {
   cancelID       MessageID                    -- MessageID est comme défini dans la [RFC2251]
}
```

Le champ cancelID contient l'identifiant de message associé à l'opération à annuler.

2.2 Réponse à Cancel

Une réponse à Cancel est une réponse étendue (ExtendedResponse) où les champs Nom de réponse (responseName) et Réponse (response) sont absents.

2.3 Codes de résultat supplémentaires

Les mises en œuvre de la présente spécification DEVRONT reconnaître les valeurs de code de résultat supplémentaires suivantes :
canceled *(annulé)* (118)
noSuchOperation *(pas de telle opération)* (119)
tooLate *(trop tard)* (120)
cannotCancel *(ne peut pas annuler)* (121)

3. Sémantique du fonctionnement

La fonction de l'opération Cancel est de demander que le serveur annule une opération en cours produite au sein de la même session.

Le client demande l'annulation d'une opération en cours en produisant une réponse Cancel avec un identifiant d'annulation (cancelID) réglé à l'identifiant de message de l'opération en cours. La demande Cancel elle-même a un identifiant de message distinct. Les clients NE DEVRAIENT PAS demander plusieurs fois l'annulation d'une opération.

Si le serveur veut, et est capable d'annuler l'opération en cours identifiée par le cancelId, le serveur DEVRA retourner une Réponse d'annulation *(Cancel Response)* avec un code de résultat de succès, et l'opération annulée DEVRA échouer avec le code de résultat de annulé. Autrement, la réponse d'annulation DEVRA avoir un code de résultat de non réussite et NE DEVRA PAS avoir un impact sur l'opération en cours (si elle existe).

Le code de résultat Erreur de protocole est retourné si le serveur n'est pas capable d'analyser la valeur de la demande ou si la valeur de la demande est absente,

Le code de résultat Pas de telle opération est retourné si le serveur n'a pas connaissance de l'opération dont l'annulation est demandée.

Le code de résultat Ne peut pas annuler est retourné si l'opération identifiée ne supporte pas l'annulation ou si l'opération d'annulation n'a pas pu être effectuée. Les classes de fonctionnement suivantes ne sont pas annulables :
- opérations qui n'ont pas de réponse,
- opérations qui créent, altèrent, ou détruisent les associations d'authentification et/ou d'autorisation,
- opérations qui établissent, altèrent, ou suppriment des services de sécurité, et
- opérations qui abandonnent ou annulent d'autres opérations.

Précisément, les opérations Abandon, Lier, Lancer TLS [RFC2830], Délier, et Cancel ne sont pas annulables.

L'opération Cancel ne peut pas être abandonnée.

Le code de résultat Trop tard est retourné pour indiquer qu'il est trop tard pour annuler l'opération en cours. Par exemple, le serveur peut retourner Trop tard pour une demande d'annulation d'une opération de modification en cours qui a déjà effectué les mises à jour de la mémorisation de données sous-jacente.

Les serveurs DEVRAIENT indiquer leur prise en charge de cette opération d'extension en fournissant 1.3.6.1.1.8 comme valeur de type d'attribut 'supportedExtension' *(attributs pris en charge)* dans leur DSE racine. Un serveur PEUT choisir de n'annoncer cette extension que lorsque le client est autorisé à l'utiliser.

4. Considérations sur la sécurité

Cette opération est destinée à permettre à un usager d'annuler des opérations qu'il a produites précédemment durant l'association LDAP en cours. Dans certains cas, comme lorsque on utilise la commande d'autorisation de mandataire, différentes opérations en cours peuvent être traitées sous différentes associations LDAP. Les serveurs NE DOIVENT PAS permettre à un usager d'annuler une opération qui appartient à un autre usager.

Certaines opérations ne devraient pas être annulables pour des raisons de sécurité. La présente spécification interdit l'annulation de l'opération Bind (*Lier)* et de l'opération d'extension Lancer TLS *(Start TLS)* afin d'éviter d'ajouter de la complexité à la sémantique d'authentification, d'autorisation, et de la couche de sécurité.

Les concepteurs de futures opérations et/ou commandes d'extension devraient interdire l'abandon et l'annulation lorsque c'est approprié.

5. Considérations relatives à l'IANA

Les valeurs suivantes ont été enregistrées par l'IANA [RFC3383].

5.1 Identifiant d'objet

L'IANA a enregistré au titre d'une action de normalisation l'identifiant d'objet LDAP 1.3.6.1.1.8 pour identifier l'opération Cancel de LDAP comme définie dans le présent document.

Sujet : Demande d'enregistrement d'identifiant d'objet LDAP
Adresse personnelle & de messagerie à contacter pour plus d'informations : Kurt Zeilenga <kurt@OpenLDAP.org>
Spécification : RFC 3909
Auteur/Contrôleur des changements : IESG
Commentaires : Identifie l'opération Cancel de LDAP

5.2 Mécanismes de protocole LDAP

L'IANA a enregistré au titre d'une action de normalisation le mécanisme de protocole LDAP décrit dans le présent document.

Sujet : Enregistrement de mécanisme du protocole LDAP
Identifiant d'objet : 1.3.6.1.1.8
Description : Opération Cancel LDAP
Adresse personnelle & de messagerie à contacter pour plus d'informations : Kurt Zeilenga <kurt@OpenLDAP.org>
Usage : Opération d'extension
Spécification : RFC 3909
Auteur/Contrôleur des changements : IESG
Commentaires : none

5.3 Codes de résultat LDAP

L'IANA a enregistré au titre d'une action de normalisation les codes de résultat LDAP décrits dans le présent document.

Sujet : Enregistrement de code de résultat LDAP
Adresse personnelle & de messagerie à contacter pour plus d'informations : Kurt Zeilenga <kurt@OpenLDAP.org>
Nom du code de résultat : annulé (118)
Nom du code de résultat : pas de telle opération (119)
Nom du code de résultat : trop tard (120)
Nom du code de résultat : ne peut pas annuler (121)
Spécification : RFC 3909
Auteur/Contrôleur des changements : IESG

6. Remerciement

L'opération Cancel de LDAP est modélisée d'après l'opération Abandon du DAP de X.511.

7. Références

7.1 Références normatives

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

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

[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.)*

[X.680] Recommandation UIT-T X.680, "Notation numéro 1 abstraite de syntaxe (ASN.1) - Spécification de la notation de base", (1997) (aussi ISO/CEI 8824-1:1998).

[X.690] Recommandation UIT-T X.690, "Spécification des règles de codage ASN.1 : Règles de codage de base (BER), Règles de codage canoniques (CER), et règles de codage distinctif (DER)", (1997) (aussi ISO/CEI 8825-1:1998).

7.2 Références pour information

[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.511] Recommandation UIT-T X.511, "L'Annuaire : Définition de service abstrait". Union Internationale des Télécommunication – Secteur de la normalisation des Télécommunications, (1993).

8. Adresse de l'auteur

Kurt D. Zeilenga
OpenLDAP Foundation

mél : Kurt@OpenLDAP.org

9. Déclaration complète de droits de reproduction

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 .

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