Groupe de travail Réseau
Request for Comments : 4522
Catégorie : Standards Track
Juin 2006

S. Legg, eB2Bcom

Traduction Claude Brière de L'Isle
mai 2007

Protocole léger d'accès à un répertoire (LDAP) : l'option de codage binaire

Statut du présent mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Notice de copyright

Résumé

Chaque attribut mémorisé dans un répertoire du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) a une syntaxe définie (c'est-à-dire, un type de données). Une définition de syntaxe spécifie comment les valeurs des attributs se conformant à la syntaxe sont normalement représentées lorsqu'elles sont transférées dans des opérations LDAP. Cette représentation est appelée le codage spécifique de LDAP pour la distinguer des autres méthodes de codage des valeurs d'attributs. Le présent document définit une option d'attribut, l'option binaire, qui peut être utilisée pour spécifier que les valeurs d'attribut associées sont codées conformément aux règles de codage de base (BER, *Basic Encoding Rules*) utilisées par les répertoires X.500.

1. Introduction

Chaque attribut mémorisé dans un répertoire du protocole léger d'accès à un répertoire (LDAP) [RFC4510] a une syntaxe définie (c'est-à-dire, un type de données) qui établit des contraintes sur la structure et le format de ses valeurs.

La description de chaque syntaxe [RFC4517] spécifie comment les valeurs d'attribut ou d'assertion [RFC4512] se conformant à la syntaxe sont normalement représentées lors du transfert dans des opérations LDAP [RFC4511]. Cette représentation est appelée le codage spécifique de LDAP pour la distinguer des autres méthodes de codage des valeurs d'attribut.

Le présent document définit une option d'attribut, l'option binaire, qui peut être utilisée dans une description d'attribut [RFC4512] d'une opération LDAP pour spécifier que les valeurs d'attribut ou valeurs d'assertion associées sont, ou qu'il leur est demandé d'être, conformes aux règles de codage de base [BER] telles qu'utilisées par les répertoires [X.500], au lieur du codages usuel spécifique de LDAP.

L'option binaire été définie à l'origine dans la RFC 2251. La spécification technique LDAP [RFC4510] a rendue obsolète la spécification technique LDAP précédemment définie [RFC3377], qui incluait la RFC 2251. L'option binaire n'était pas incluse dans la spécification technique LDAP révisée pour une série de raison qui incluent des incohérences de mise en oeuvre. On n'a pas cherché ici à résoudre les incohérences découvertes.

Le présent document réintroduit l'option binaire à utiliser avec certaines syntaxes d'attribut, comme la syntaxe de certificat [RFC4523], qui l'exige spécifiquement. Aucune tentative n'a été faite pour traiter l'utilisation de l'option binaire avec les attributs de syntaxes qui n'exigent pas son utilisation. Sauf si c'était traité dans une spécification future, cette utilisation devrait être évitée.

2. Conventions

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

3. L'option binaire

L'option binaire est indiquée par la chaîne d'option d'attribut "binary" dans une description d'attribut. Noter que, comme toutes les options d'attribut, la chaîne représentant l'option binaire est insensible à la casse.

Lorsque l'option binaire est présente dans une description d'attribut, les valeurs d'attribut ou valeurs d'assertion associées DOIVENT être codées en BER (autrement, les valeurs sont codée conformément au codage spécifique de LDAP [RFC4517] pour la syntaxe de l'attribut). Noter qu'il est possible qu'une syntaxe soit définie de telle sorte que son codage spécifique de LDAP soit exactement le même que son codage en BER.

En termes de protocole [RFC4511], l'option binaire spécifie que les octets de contenu de la CHAINE D'OCTET valeur d'attribut ou valeur d'assertion associée sont un codage BER complet de la valeur pertinente.

L'option binaire n'est pas une option d'étiquetage [RFC4512], aussi la présence de l'option binaire ne spécifie pas un sous-type d'attribut. Une description d'attribut qui contient l'option binaire fait référence exactement au même attribut que la description d'attribut sans l'option binaire. Les relations de super-type/sous-type des attributs avec des options d'étiquetage ne sont altérées en aucune façon par la présence ou l'absence de l'option binaire.

Une description d'attribut DOIT être traitée comme non reconnue si elle contient l'option binaire et si la syntaxe de l'attribut n'a pas un type ASN.1 [RFC4517] associé, ou si le codage en BER des valeurs de ce type n'est pas pris en charge.

La présence ou l'absence de l'option binaire n'affecte que le transfert des valeurs d'attribut et d'assertion dans le protocole ; les serveurs mémorisent toute valeur d'attribut particulière dans le format de leur choix.

4. Syntaxes exigeant le transfert binaire

Les valeurs d'attribut de certaines syntaxes d'attribut sont définies sans un codage spécifique de LDAP et il est exigé qu'elles soient transférées sous la forme codée en BER. Pour les besoins du présent document, ces syntaxes sont dites avoir une exigence de transfert binaire. Les syntaxes de certificat, de liste de certificat, de paire de certificat, et d'algorithmes pris en charge [RFC4523] sont des exemples de syntaxes avec une exigence de transfert binaire. Ces syntaxes ont aussi une exigence supplémentaire que le codage BER exact soit préservé. Noter que ceci est une propriété des syntaxes elles-mêmes, et non une propriété de l'option binaire. En l'absence de cette exigence, les clients LDAP auraient besoin de recoder les valeurs en utilisant les règles de codage distinctif (DER).

5. Attributs retournés dans une recherche

Une demande de recherche LDAP [RFC4511] contient une liste des attributs (la liste des attributs demandés) à retourner à partir de chaque entrée qui correspond au filtre de recherche. Une description d'attribut dans la liste d'attributs demandés demande aussi implicitement tous les sous-types du type d'attribut dans la description d'attribut, que ce soit par des sous-types d'attribut ou par des sous-types d'option d'étiquetage d'attribut [RFC4512].

La liste des attributs demandés PEUT contenir des descriptions d'attribut avec l'option binaire, mais NE DOIT PAS contenir deux descriptions d'attribut avec le même type d'attribut et les mêmes options d'étiquetage (même si seulement une d'entre elles a l'option binaire). L'option binaire dans une description d'attribut au sein de la liste d'attributs demandée s'applique implicitement à tous les sous-types du type d'attribut dans la description d'attribut (voir cependant à la Section 7).

S'ils sont retournés, les attributs d'une syntaxe avec l'exigence de transfert binaire DOIVENT être retournés en forme binaire (c'est-à-dire, avec l'option binaire dans la description d'attribut et les valeurs d'attribut associées codées en BER) que l'option binaire soit ou non présente dans la demande (pour l'attribut ou pour un de ses super-types).

Les attributs d'une syntaxe sans l'exigence de transfert binaire, s'ils sont retournés, DEVRAIENT être retournés sous la forme explicitement demandée. C'est à dire que si la description d'attribut dans la liste des attributs demandés contient l'option binaire, l'attribut correspondant dans le résultat DEVRAIT être en forme binaire. Si la description d'attribut dans la demande ne contient pas l'option binaire, l'attribut correspondant dans le résultat NE DEVRAIT PAS alors être en forme binaire. Un serveur PEUT omettre un attribut dans le résultat si il n'accepte pas le codage demandé.

Quel que soit le codage choisi, une valeur d'attribut particulière est retournée au plus une fois.

6. Attributs tous utilisateurs

Si la liste des attributs dans une demande de recherche est vide ou contient la chaîne spéciale de description d'attribut "*", il est alors demandé de retourner tous les attributs d'utilisateur.

Les attributs d'une syntaxe avec l'exigence de transfert binaire, s'ils sont retournés, DOIVENT être retournés sous la forme binaire.

Les attributs d'une syntaxe qui n'a pas l'exigence du transfert binaire et qui a un codage spécifique de LDAP défini NE DEVRAIENT PAS être retournés sous forme binaire.

Les attributs d'une syntaxe qui n'a pas l'exigence du transfert binaire et qui n'a pas de codage spécifique de LDAP défini peuvent être retournés sous la forme binaire ou omis du résultat.

7. Demandes contradictoires

Un attribut particulier pourrait être demandé explicitement par une description d'attribut et/ou implicitement demandé par les descriptions d'attribut d'un ou plusieurs de ses super-types, ou par la chaîne spéciale de description d'attribut "*". Si l'option binaire est présente dans au moins un, mais pas toutes, ces descriptions d'attribut, l'effet de la demande sur le transfert binaire est défini par la mise en œuvre.

8. Considérations sur la sécurité

En interprétant les champs sensibles à la sécurité, et en particulier les champs utilisés pour accorder ou refuser l'accès, les mises en oeuvre DOIVENT s'assurer que toutes les comparaisons de règles de correspondance sont effectuées sur la valeur abstraite sous-jacente, indépendamment du codage particulier utilisé.

9. Considérations relatives à l'IANA

L'autorité d'allocation des numéros de l'Internet (IANA) a mis à jour le registre LDAP d'option de description d'attribut [BCP64] comme indiqué par le modèle suivant :

Sujet : Demande d'enregistrement d'option de description d'attribut LDAP
Nom de l'option : binaire
Famille d'options : AUCUNE
Adresse personnelle et de messagerie du contact pour des précisions : Steven Legg <steven.legg@eb2bcom.com>
Spécification : RFC 4522
Auteur/Contrôleur des modifications : IESG

10. Références

10.1 Références normatives

[BCP14] Bradner, S., "Mots clé à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[BCP64] Zeilenga, K., "Autorité d'allocation des numéros de l'Internet (IANA) : Considérations sur le Protocole léger d'accès de répertoire (LDAP)", BCP 64, RFC 4520, juin 2006.

[RFC4510] Zeilenga, K., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Descriptif des spécifications techniques", RFC 4510, juin 2006.

[RFC4511] Sermersheim, J., Ed., "Protocole léger d'accès à un répertoire (LDAP) Le protocole", RFC 4511, juin 2006.

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

[RFC4517] Legg, S., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Syntaxes et règles de correspondance", RFC 4517, juin 2006.

[RFC4523] Zeilenga, K., "Protocole léger d'accès à un répertoire (LDAP) : Définitions de schémas pour les certificats X.509", RFC 4523, juin 2006.

[BER] Recommandation UIT-T X.690 (07/02) | ISO/CEI 8825-1, Technologies de l'information – règles de codage ASN.1 : Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER).

10.2 Références informatives

[RFC2251] Wahl, M., Howes, T., et S. Kille, "Protocole léger d'accès à un répertoire (v3)", RFC 2251, décembre 1997.

[RFC3377] Hodges, J. et R. Morgan, "Protocole léger d'accès à un répertoire (v3): Spécification technique", RFC 3377, septembre 2002.

[X.500] Recommandation UIT-T X.500 (02/01) | ISO/CEI 9594-1:2001, Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire : Vue d'ensemble des concepts, modèles et services.

Adresse de l'auteur

Dr. Steven Legg
eB2Bcom
Suite 3, Woodhouse Corporate Centre
935 Station Street
Box Hill North, Victoria 3129
AUSTRALIA
téléphone : +61 3 9896 7830
fax : +61 3 9896 7801
mél : steven.legg@eb2bcom.com

Déclaration de copyright

Propriété intellectuelle

Des copies des dépôts d’IPR faites au secrétariat de l’IETF et toutes assurances de disponibilité de licences, ou le résultat de 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 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.

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