Groupe de travail Réseau
Request for Comments : 4514
RFC rendues obsolètes : 2253
Catégorie : Norme

K. Zeilenga, OpenLDAP Foundation
01/06/06
Traduction Claude Brière de L'Isle
décembre 2006

Protocole léger d'accès à un répertoire (LDAP) : Représentation de chaîne des noms distinctifs

Statut de ce 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.

Résumé

L'annuaire X.500 utilise les noms distinctifs (DN, *Distinguinshed Names*) comme clés principales pour les entrées dans le répertoire. Le présent document définit la représentation de chaîne utilisée dans le protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) pour le transfert des noms distinctifs. La représentation de chaîne est destinée à donner une représentation claire des noms distinctifs communément utilisés, tout en étant capable de représenter tout nom distinctif.

1 Fondements et destination

Dans les systèmes de répertoire fondés sur X.500, y compris ceux auxquels on accède en utilisant le protocole léger d'accès à un répertoire (LDAP) [RFC4510], les noms distinctifs (DN) sont utilisés pour se référer de façon non ambiguë aux entrées du répertoire [X.501] [RFC4512].

La structure d'un DN [X.501] est décrite en termes d'ASN.1 [X.680]. Dans le Protocole d'accès à l'annuaire X.500 [X.511] (et autres protocoles de répertoire définis par l'UIT-T), les noms distinctifs sont codés en utilisant les règles de codage de base (BER, *Basic Encoding Rules*) [X.690]. Dans LDAP, les DN sont représentés sous la forme de chaînes décrite dans le présent document.

Il est important d'avoir un format commun pour être capable de représenter de façon non ambiguë un nom distinctif. Le principal objectif de la présente spécification est de faciliter le codage et le décodage Un objectif secondaire est d'avoir des noms lisibles par l'homme. On ne s'attend pas à ce que les mises en œuvre de LDAP avec une interface d'utilisateur humain affichent ces chaînes directement à l'utilisateur, mais à ce qu'elles fassent vraisemblablement des traductions (comme d'exprimer des noms de type d'attribut dans la langue nationale locale).

Le présent document définit la représentation de chaîne des noms distinctifs utilisés dans LDAP [RFC4511] [RFC4517]. La Section 2 détaille l'algorithme RECOMMANDÉ pour la conversion d'un DN depuis sa représentation structurée en ASN.1 en une chaîne. La Section 3 détaille la façon de convertir un DN depuis une chaîne en une représentation structurée ASN.1.

Alors que d'autres documents peuvent définir d'autres algorithmes de conversion d'un DN de sa représentation structurée ASN.1 en une chaîne, tous les algorithmes DOIVENT produire des chaînes qui adhèrent aux exigences de la Section 3.

Le présent document ne définit pas de représentation canonique de chaîne pour les DN. La comparaison pour égalité des noms distinctifs doit être effectuée conformément à la règle de correspondance distinguishedNameMatch [RFC4517].

Le présent document fait partie intégrante de la spécification technique LDAP [RFC4510], qui rend obsolète la spécification technique LDAP précédemment définie, RFC 3377, dans sa totalité. Le présent document rend obsolète la RFC 2253. Les changements depuis la RFC 2253 sont résumés à l'Appendice B.

La présente spécification suppose une certaine familiarité avec X.500 [X.500] et le concept de nom distinctif [X.501] [RFC4512].

1.1 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].

Dans le présent document, les noms de caractères utilisent la notation des codets et des noms d'après la norme [Unicode]. Par exemple, la lettre "a" peut être représentée par <U+0061> ou <LETTRE LATINE A MINUSCULE>.

Note : un glossaire des termes utilisés en Unicode se trouve dans [Glossary]. On trouvera des informations sur le modèle de codage de caractères Unicode dans [CharModel].

2 Conversion de DistinguishedName d'ASN.1 en chaîne

La Recommandation UIT-T X.501 définit la structure ASN.1 [X.680] d'un nom distinctif. Ce qui suit est une variante fournie pour les besoins de l'exposé.

```
DistinguishedName ::= RDNSequence
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::= SET SIZE (1..MAX) OF
        AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
        type  AttributeType,
        value AttributeValue }
```

La présente section définit l'algorithme RECOMMANDÉ pour la conversion d'un nom distinctif d'une représentation structurée ASN.1 en représentation de chaîne de caractères Unicode codés en UTF-8 [RFC3629]. D'autres documents peuvent décrire d'autres algorithmes pour la conversion d'un nom distinctif en chaîne, mais seules les chaînes qui se conforment à la grammaire définie à la Section 3 DOIVENT être produites par les mises en œuvre LDAP.

2.1 Conversion de RDNSequence

Si la RDNSequence est une séquence vide, le résultat est la chaîne vide ou de longueur zéro.

Autrement, le résultat consiste en les codages de chaîne de chaque RelativeDistinguishedName dans la RDNSequence (conformément au paragraphe 2.2), commençant par le dernier élément de la séquence et en reculant jusqu'au premier.

Les codages des RelativeDistinguishedNames joints sont séparés par un caractère virgule (',' U+002C).

2.2 Conversion de RelativeDistinguishedName

Lors de la conversion d'un RelativeDistinguishedName d'ASN.1 en chaîne, le résultat consiste en les codages de chaîne de chaque AttributeTypeAndValue (conformément au paragraphe 2.3), dans n'importe quel ordre.

Lorsqu'il y a un RDN multi valeurs, les résultats de AttributeTypeAndValues joints sont séparés par un caractère signe plus ('+' U+002B).

2.3 Conversion de AttributeTypeAndValue

AttributeTypeAndValue est codé comme la représentation de chaîne de AttributeType, suivi par un caractère signe égal ('=' U+003D), suivi par la représentation de chaîne de AttributeValue. Le codage de AttributeValue est donné au paragraphe 2.4.

Si le AttributeType est défini comme ayant un nom abrégé (descripteur) [RFC4512] et si le nom abrégé est connu pour être enregistré [REGISTRY] [RFC4520] comme identifiant de AttributeType, ce nom abrégé, un <descr>, est utilisé. Autrement le AttributeType est codé comme le codage décimal à octets séparés par des points, un <numericoid>, de son OBJECT IDENTIFIER. Le <descr> et le <numericoid> sont définis dans la [RFC4512].

Les mises en œuvre ne sont pas supposées mettre à jour de façon dynamique leur connaissance des noms abrégés enregistrés. Cependant, les mises en œuvre DEVRAIENT fournir un mécanisme permettant de mettre à jour leur connaissance des noms abrégés enregistrés.

2.4 Conversion de AttributeValue d'ASN.1 en chaîne

Si le AttributeType est de forme décimale à séparation des octets par des points, la AttributeValue est représentée par un caractère signe dièse ('#' U+0023) suivi par le codage en hexadécimal de chacun des octets du codage en BER de la AttributeValue X.500. Cette forme est aussi utilisée lorsque la syntaxe de AttributeValue n'a pas de codage de chaîne spécifique de LDAP ([RFC4517], paragraphe 3.1) défini pour elle, ou si le codage de chaîne spécifique de LDAP n'est pas restreint aux caractères Unicode codés en UTF-8. Cette forme peut aussi être utilisée dans d'autres cas, tels que lorsque on désire une représentation réversible de chaîne (voir au paragraphe 5.2).

Autrement, si la AttributeValue est d'une syntaxe qui a un codage de chaîne spécifique de LDAP, la valeur est convertie d'abord en chaîne Unicode codée en UTF-8 conformément à sa spécification de syntaxe (voir des exemples au paragraphe 3.3 de la [RFC4517]). Si cette chaîne Unicode codée en UTF-8 n'a aucun des caractères suivants qui doive être codé en pourcentage (*"échappé"*), cette chaîne peut alors être utilisée comme la représentation de chaîne de la valeur.

- un espace (' ' U+0020) ou le signe dièse ('#' U+0023) survenant au début de la chaîne,
- un caractère espace (' ' U+0020) survenant à la fin de la chaîne,
- un des caractères '"', '+', ',', ';', '<', '>', ou '\' (respectivement, U+0022, U+002B, U+002C, U+003B, U+003C, U+003E, ou U+005C),
- le caractère nul (U+0000).

Les autres caractères peuvent être codés en pourcentage.

Chaque octet du caractère à coder en pourcentage est remplacé par une barre oblique inversée '\' et deux chiffres hexadécimaux, qui forment un seul octet dans le code du caractère. Autrement, si et seulement si le caractère à coder en pourcentage est un des suivants : ' ', '"', '#', '+', ',', ';', '<', '=', '>', ou '\' (respectivement, U+0020, U+0022, U+0023, U+002B, U+002C, U+003B, U+003C, U+003D, U+003E, U+005C), il peut avoir en préfixe une barre oblique inversée ('\' U+005C).

Des exemples du mécanisme de codage en pourcentage sont donnés à la Section 4.

3 Analyse grammaticale du retour d'une chaîne à un nom distinctif

La représentation de chaîne des noms distinctifs est restreinte aux caractères Unicode codés en UTF-8 [RFC3629]. La structure de cette représentation de chaîne est spécifiée en utilisant la grammaire BNF augmentée [RFC4234] suivante :

```
distinguishedName = [ relativeDistinguishedName
        *( COMMA relativeDistinguishedName ) ]
relativeDistinguishedName = attributeTypeAndValue
        *( PLUS attributeTypeAndValue )
attributeTypeAndValue = attributeType EQUALS attributeValue
attributeType = descr / numericoid
attributeValue = string / hexstring
```

; Les caractères suivants sont à coder en pourcentage lorsqu'ils apparaissent dans la valeur à coder : ESC, un des <escaped>, SHARP ou SPACE en tête, SPACE en queue, et NULL.
string = [(leadchar / pair) [*(stringchar / pair) (trailchar / pair)]]
leadchar = LUTF1 / UTFMB LUTF1 = %x01-1F / %x21 / %x24-2A / %x2D-3A / %x3D / %x3F-5B / %x5D-7F
trailchar = TUTF1 / UTFMB TUTF1 = %x01-1F / %x21 / %x23-2A / %x2D-3A / %x3D / %x3F-5B / %x5D-7F
stringchar = SUTF1 / UTFMB SUTF1 = %x01-21 / %x23-2A / %x2D-3A / %x3D / %x3F-5B / %x5D-7F
pair = ESC (ESC / special / hexpair)
special = escaped / SPACE / SHARP / EQUALS
escaped = DQUOTE / PLUS / COMMA / SEMI / LANGLE / RANGLE
hexstring = SHARP 1*hexpair
hexpair = HEX HEX

où les produits <descr>, <numericoid>, <COMMA>, <DQUOTE>, <EQUALS>, <ESC>, <HEX>, <LANGLE>, <NULL>, <PLUS>, <RANGLE>, <SEMI>, <SPACE>, <SHARP>, et <UTFMB> sont définis dans la [RFC4512].

Chaque <attributeType>, soit un <descr> soit un <numericoid>, se réfère à un type d'attribut d'une assertion de valeur d'attribut (AVA, *attribute value assertion*). Le <attributeType> est suivi par un <EQUALS> et un <attributeValue>. Le <attributeValue> est soit en forme <string> soit en <hexstring>.

Si elle est en forme <string>, une valeur affirmée de représentation de chaîne LDAP peut être obtenue en remplaçant (de gauche à droite, sans récurrence) chaque <pair> apparaissant dans la <string> comme suit :

remplacer <ESC><ESC> par <ESC>;
remplacer <ESC><special> par <special>;
remplacer <ESC><hexpair> par l'octet indiqué par la <hexpair>.

Si elle est en forme <hexstring>, une représentation en BER peut être obtenue de la conversion de chaque <hexpair> de la <hexstring> en l'octet indiqué par la <hexpair>.

Il y a une ou plusieurs assertions de valeur d'attribut, séparées par <PLUS>, pour un nom distinctif relatif.

Il y a zéro, un ou plusieurs noms distinctifs relatifs, séparés par <COMMA>, pour un nom distinctif.

Les mises en œuvre DOIVENT reconnaître les chaînes de nom AttributeType (descripteurs) dont la liste figure dans les tableaux suivants, mais PEUVENT reconnaître d'autres chaînes de noms.

String	X.500 AttributeType
CN	commonName (2.5.4.3)
L	localityName (2.5.4.7)
ST	stateOrProvinceName (2.5.4.8)
O	organizationName (2.5.4.10)
OU	organizationalUnitName (2.5.4.11)
C	countryName (2.5.4.6)
STREET	streetAddress (2.5.4.9)
DC	domainComponent (0.9.2342.19200300.100.1.25)
UID	userId (0.9.2342.19200300.100.1.1)

Ces types d'attribut sont décrits dans la [RFC4519].

Les mises en œuvre PEUVENT reconnaître d'autres représentations de chaînes de DN. Cependant, comme il n'y a pas d'exigence que d'autres représentations de chaînes de DN soient reconnues (et, s'il en est ainsi, sur la façon de le faire) les mises en œuvre DEVRAIENT seulement générer des chaînes de DN conformément à Section 2 du présent document.

4 Exemples

Cette notation est conçue pour convenir aux formes communes des noms. La présente section donne quelques exemples de noms distinctifs écrits en utilisant cette notation. Tout d'abord, figure un nom qui contient trois noms distinctifs relatifs (RDN) :

UID=jsmith,DC=example,DC=net

Ensuite voici un exemple de nom contenant trois RDN, dans lequel le premier RDN est multi valeurs :

OU=Sales+CN=J. Smith,DC=example,DC=net

L'exemple suivant montre la méthode d'échappement de caractères spéciaux qui apparaissent dans un nom commun :

CN=James \"Jim\" Smith\, III,DC=example,DC=net

L'exemple ci-après montre la méthode de codage d'une valeur qui contient un caractère retour chariot :

CN=Before\0dAfter,DC=example,DC=net

Dans l'exemple de RDN suivant, le type dans le RDN n'est pas reconnu, et la valeur est le codage en BER d'une CHAINE D'OCTET contenant deux octets, 0x48 et 0x69.

1.3.6.1.4.1.1466.0=#04024869

Enfin, l'exemple suivant montre un RDN dont la valeur commonName consiste en cinq lettres :

Caractère Unicode	**Code**	**UTF-8**	**Echappé**
LETTRE LATINE L MAJUSCULE	U+004C	0x4C	L
LETTRE LATINE U MINUSCULE	U+0075	0x75	u
LETTRE LATINE C MINUSCULE AVEC CARON	U+010D	0xC48D	\C4\8D
LETTRE LATINE I MINUSCULE	U+0069	0x69	i
LETTRE LATINE C MINUSCULE AVEC ACCENT AIGU	U+0107	0xC487	\C4\87

Ceci pourrait être codé en ASCII imprimable (utile pour les besoins du déboguage) comme :

CN=Lu\C4\8Di\C4\87

5 Considérations sur la sécurité

Les considérations suivantes sur la sécurité sont spécifiques du traitement des noms distinctifs. Les considérations LDAP sur la sécurité sont exposées dans la [RFC4511] et d'autres documents qui composent la spécification technique LDAP [RFC4510].

5.1 Divulgation

Les noms distinctifs consistent normalement en informations descriptives sur les entrées qu'ils nomment, qui peuvent être des personnes, des organisations, des appareils, ou autres objets du monde réel. Cela inclut fréquemment certaines des sortes d'informations suivantes :

- le nom commun de l'objet (c'est-à-dire, le nom complet d'une personne)
- une adresse de messagerie électronique ou TCP/IP
- sa localisation physique (pays, localité, ville, adresse dans la rue)
- des attributs organisationnels (tels que le nom d'un bureau ou l'appartenance)

Dans certains cas, de telles informations peuvent être considérées comme sensibles. Dans de nombreux pays, il existe des lois sur la confidentialité qui interdisent la divulgation de certaines sortes d'informations descriptives (par exemple, des adresses de messagerie électronique). Et donc, les développeurs de serveurs sont encouragés à prendre en charge les règles structurelles et les formes de nom d'arborescence d'informations de répertoire (DIT, *Directory Information Tree*) de la [RFC4512], car elles fournissent aux administrateurs un mécanisme pour choisir les attributs de dénomination appropriés pour les entrées. Les administrateurs sont encouragés à utiliser les mécanismes, contrôles d'accès, et autres contrôles administratifs qui peuvent être disponibles pour restreindre l'utilisation des attributs qui contiennent des informations sensibles dans les dénominations d'entrées. De plus, l'utilisation de services d'authentification et de sécurité des données de LDAP [RFC4513][RFC4511] devrait être envisagée.

5.2 Utilisation des noms distinctifs dans les applications de sécurité

Les transformations d'une valeur d'un AttributeValue à partir de sa forme X.501 en représentation de chaîne LDAP ne sont pas toujours réversibles à la même forme de BER (règles de codage de base) ou DER (règles de codage distinctif). L'exemple d'une situation qui exige la forme DER de nom distinctif est la vérification d'un certificat X.509.

Par exemple, un nom distinctif consistant en un RDN avec une AVA, dans lequel le type est commonName et la valeur est le choix TeletexString avec les lettres 'Sam', serait représenté en LDAP par la chaîne <CN=Sam>. Un autre nom distinctif dans lequel la valeur est toujours 'Sam', mais où le choix est PrintableString, aurait la même représentation <CN=Sam>.

Les applications qui exigent la reconstruction de la forme DER de la valeur NE DEVRAIENT PAS utiliser la représentation de chaîne des syntaxes d'attribut lors de la conversion d'un nom distinctif en format LDAP. À la place, elles DEVRAIENT utiliser la forme hexadécimale avec en préfixe le signe dièse ('#' U+0023) comme décrit au premier alinéa du paragraphe 2.4.

6 Remerciements

Le présent document est une mise à jour de la RFC 2253, par Mark Wahl, Tim Howes, et Steve Kille. La RFC 2253 a été produite par le groupe de travail ASID de l'IETF.

Le présent document a été produit par le groupe de travail LDAPBIS de l'IETF.

7 Références

7.1 Références normatives

[REGISTRY] IANA, Object Identifier Descriptors Registry *(Registre des descripteurs d'identifiants d'objet)*, <http://www.iana.org/assignments/ldap-parameters>.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" *(Norme Unicode, version 3.2.0)* est définie par "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), telle qu'amendée par "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) et par "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

[X.501] Union internationale des télécommunications — Secteur de la normalisation des télécommunications, "Technologies de l'information — Interconnexion des systèmes ouverts — L'annuaire : les modèles", (1993) (aussi ISO/IEC 9594-2:1994).

[X.680] Union internationale des télécommunications — Secteur de la normalisation des télécommunications, "Notation de syntaxe abstraite n° 1 (ASN.1) - Spécification de la notation de base", (1997) (aussi ISO/CEI 8824-1:1998).

[RFC2119] Bradner, S., "Mots clé à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.
[RFC3629] Yergeau, F., "UTF-8, un format de transformation de ISO 10646", STD 63, RFC 3629, novembre 2003.
[RFC4234] Crocker, D. et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", RFC 4234, octobre 2005.
[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.

[RFC4513] Harrison, R., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Méthodes d'authentification et mécanismes de sécurité", RFC 4513, juin 2006.
[RFC4517] Legg, S., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Syntaxes et règles de correspondance", RFC 4517, juin 2006.
[RFC4519] Sciberras, A., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Schéma pour les applications d'utilisateur", RFC 4519, juin 2006.
[RFC4520] 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.

7.2 Références informatives

[ASCII] Coded Character Set--7-bit American Standard Code for Information Interchange, ANSI X3.4-1986.

[CharModel] Whistler, K.et M. Davis, "Rapport technique Unicode n° 17, Modèle de codage de caractères", UTR17, <http://www.unicode.org/unicode/reports/tr17/>, août 2000.

[Glossary] The Unicode Consortium, "Glossaire Unicode", <http://www.unicode.org/glossary/>.

[X.500] Union Internationale des Télécommunications – Secteur de la normalisation des télécommunications, "L'annuaire – Vue générales des concepts, modèles et services," (1993) (aussi ISO/IEC 9594-1:1994).

[X.511] Union Internationale des Télécommunications – Secteur de la normalisation des télécommunications, "L'annuaire – Définition du service abstrait", (1993) (aussi ISO/IEC 9594-3:1993).

[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 canoniques (CER), et Règles de codage distinctives (DER)", (1997) (aussi ISO/IEC 8825-1:1998).

[RFC2849] Good, G., "Le format d'échange de données LDAP (LDIF) – Spécification technique", RFC 2849, juin 2000.

Appendice A Questions de présentation

Le présent appendice est fourni uniquement pour des besoins d'information ; il n'est pas une partie normative de la présente spécification.

La représentation de chaîne décrite dans ce document n'est pas destinée à être présentée sans traduction aux personnes humaines. Cependant, il peut être souhaitable à certains moments de présenter des chaînes de DN non traduites aux utilisateurs. La présente section expose les questions de présentation associées aux chaînes de DN non traduites. Les questions de présentation des chaînes de DN traduites ne sont pas discutées dans cet appendice. Les questions de transcodage ne sont pas non plus discutées dans cet appendice.

Le présent appendice donne des lignes directrices pour les applications qui présentent des chaînes de DN aux utilisateurs. Cette section n'est pas exhaustive ; elle ne discute pas de toutes les questions de présentation auxquelles peuvent faire face les développeurs.

Toutes les interfaces d'utilisateur ne sont pas capables d'afficher l'ensemble complet des caractères Unicode. Certains caractères Unicode ne sont pas affichables.

Il est recommandé que les interfaces humaines utilisent le mécanisme facultatif d'échappement de paire hexadécimale (paragraphe 2.3) pour produire une représentation de chaîne convenable pour l'affichage à l'utilisateur. Par exemple, une application peut générer une chaîne de DN à l'affichage qui code en pourcentage ("échappe") tous les caractères non imprimables qui apparaissent dans la représentation de chaîne de la AttributeValue (comme montré dans l'exemple final de la Section 4).

Lorsqu'une chaîne de DN est affichée en texte de forme libre, il est souvent nécessaire de distinguer la chaîne de DN du texte environnant. Alors que cela est souvent fait avec des espaces blancs *(whitespace)* (comme montré à la

Section 4), il est noté que les chaînes de DN peuvent se terminer par des espaces blancs. Les lecteurs attentifs de la Section 3 auront noté que les caractères '<' (U+003C) et '>' (U+003E) ne peuvent apparaître dans la chaîne de DN que s'ils sont codés en pourcentage. Ces caractères sont destinés à être utilisés en texte à forme libre pour distinguer une chaîne de DN du texte environnant. Par exemple, <CN=Sam\ > distingue la représentation de chaîne du DN composé d'un RDN consistant en l'AVA (la valeur du commonName (CN) 'Sam ') du texte environnant. Il vaut de noter pour l'utilisateur que les caractères d'enveloppement '<' et '>' ne font pas partie de la chaîne de DN.

Les chaînes de DN peuvent être assez longues. Il est souvent souhaitable de renvoyer à la ligne les chaînes de DN trop longues dans les présentations. Le renvoi à la ligne devrait être effectué par l'insertion d'une espace après le caractère séparateur de RDN ou, si nécessaire, après le caractère séparateur d'AVA. Il faut signaler à l'utilisateur que l'espace insérée ne fait pas partie de la chaîne de DN et qu'elle est à retirer avant l'utilisation dans LDAP. Par exemple, la chaîne de DN suivante est trop longue :

```
CN=Kurt D.  Zeilenga,OU=Engineering,L=Redwood Shores,
O=OpenLDAP Foundation,ST=California,C=US
```

Elle a donc subie une coupure de ligne pour sa lisibilité. L'espace est à retirer avant l'utilisation de la chaîne de DN dans LDAP.

Insérer des espaces n'est pas conseillé parce qu'il peut ne pas apparaître à l'évidence pour l'utilisateur quelle espace fait partie de la chaîne de DN et quelle espace a été ajoutée pour la lisibilité.

Une autre solution est d'utiliser le format d'échange de données LDAP (LDIF, *LDAP Data Interchange Format*) [RFC2849]. Par exemple :

```
# Cette entrée a un long nom distinctif...
dn: CN=Kurt D.  Zeilenga,OU=Engineering,L=Redwood Shores,
O=OpenLDAP Foundation,ST=California,C=US
CN: Kurt D.  Zeilenga
SN: Zeilenga
objectClass: person
```

Appendice B Changements depuis la RFC 2253

Le présent appendice n'est donné qu'à des fins d'information, il n'est pas une partie normative de cette spécification.

Les changements de substance suivants ont été faits à la RFC 2253 :

- Retrait de la note IESG. La note IESG a été traitée.
- Remplacement de toutes les références à ISO 10646-1 par [Unicode].
- Précision (Section 1) que ce document ne définit pas une représentation de chaîne canonique.
- Précision que la Section 2 décrit l'algorithme de codage RECOMMANDÉ et que des algorithmes de remplacement sont admis. Certaines options de codage décrites dans la RFC 2253 sont maintenant traitées comme des algorithmes de remplacement dans cette spécification.
- Révision de la spécification (Section 2) pour permettre aux noms abrégés de tout type d'attribut enregistré d'apparaître dans une représentation de chaîne de DN au lieu d'être restreints à un "tableau publié". Suppression de l'expression "à titre d'exemple". Ajout d'une déclaration (Section 3) permettant la reconnaissance de noms supplémentaires mais exigeant la reconnaissance de ces noms dans le tableau publié. Le tableau apparaît maintenant à la Section 3.
- Suppression de la spécification d'exigences supplémentaires pour les mises en œuvre de LDAPv2 qui prennent aussi en charge LDAPv3 (RFC 2253, Section 4) car LDAPv2 est maintenant dépassé.
- Permet la reconnaissance d'autres représentations de chaîne.
- Mise à jour du paragraphe 2.4 pour permettre l'échappement de tous les caractères par une paire hexadécimale et précision de l'échappement lorsque sont présents des codages UTF-8 à plusieurs octets. Indication que le caractère nul (U+0000) est à échapper. Indiqué que le caractère signe égal ('=' U+003D) peut être échappé par '\='.
- Réécriture de la Section 3 pour utiliser l'ABNF comme défini dans la RFC 4234.
- Mise à jour de l'ABNF de la Section 3. Les changements incluent :
  + admission des noms abrégés de AttributeType de longueur 1 (par exemple, 'L'),
  + utilisation d'une production d<oid> plus restrictive dans AttributeTypes,
  + ne pas exiger l'échappement du caractère signe égal ('=' U+003D),
  + ne pas exiger l'échappement des caractère dièse ('#' U+0023) lorsqu'il n'est pas en tête,
  + admettre que l'espace (' ' U+0020) soit échappé par '\ ',
  + exiger l'échappement hexadécimal des caractères nul (U+0000), et
  + suppression des constructions en LDAPv2 seul.
- Mise à jour de la Section 3 pour décrire comment analyser les éléments de la grammaire.
- Réécriture des exemples.
- Ajout de références aux documentations contenant des considérations générales LDAP sur la sécurité.
- Ajout de la discussion des questions de présentation (Appendice A).
- Ajout du présent appendice.

De plus, de nombreux changements rédactionnels ont été effectués.

Adresse de l'éditeur

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

Déclaration de copyright

GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible o pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

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.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif de l'IETF (IASA, *Administrative Support Activity*).