Groupe de travail Réseau
Request for Comments : 2247
Catégorie : En cours de normalisation

S. Kille, Isode Ltd.
M. Wahl, Critical Angle Inc.
A. Grimstad, AT&T
R. Huber, AT&T
S. Sataluri, AT&T

Traduction Claude Brière de L'Isle
janvier 1998

Utilisation des domaines dans les noms distinctifs LDAP/X.500

1. Résumé

Le protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) utilise les noms distinctifs compatibles avec X.500 [3] pour fournir une identification univoque des entrées.

Le présent document définit un algorithme par lequel un nom enregistré auprès du service des noms de domaines de l'Internet [2] peut être représenté comme un nom distinctif LDAP.

2. Fondements

Le système des serveurs de noms de domaine (DNS, *Domain Nameserver System*) est un système d'étiquetage hiérarchique des ressources. Un nom est constitué d'un ensemble ordonné de composants, dont chacun est fait de courtes chaînes. Un exemple de nom de domaine avec deux composants serait "CRITICAL-ANGLE.COM".

Les répertoires fondés sur LDAP donnent un cadre plus général de désignations hiérarchisées. La principale différence de spécification entre les noms distinctifs et les noms de domaines est que chaque composant d'un nom distinctif a une indication explicite de type d'attribut.

X.500 ne rend pas obligatoire de structure de désignation particulière. Il contient bien des structures de désignation suggérées qui sont fondées sur les régions géographiques et nationales, mais il n'y a cependant pas actuellement d'infrastructure d'enregistrement établie dans de nombreuses régions qui seraient capables d'allouer ou d'assurer des noms univoques.

Le mécanisme décrit dans le présent document fournit automatiquement à une entreprise un nom distinctif pour chaque nom de domaine dont elle a obtenu l'usage dans l'Internet. Ces noms distinctifs peuvent être utilisés pour identifier des objets dans un répertoire LDAP.

Un exemple de nom distinctif représenté dans le format de chaîne LDAP [3] est "DC=CRITICAL-ANGLE,DC=COM". Comme avec un nom de domaine, le composant le plus significatif, terminé par la racine de l'espace de nom, est écrit en dernier.

Le présent document ne définit pas comment représenter les objets qui n'ont pas de nom de domaine. Pas plus qu'il ne définit la procédure pour localiser le serveur de répertoire LDAP d'une entreprise, connaissant son nom de domaine. De telles procédures pourront être définies dans des RFC futures.

3. Transposition de noms de domaines en noms distinctifs

Cette section définit un sous-ensemble des structures possibles de noms distinctifs à utiliser pour représenter les noms alloués dans le système des noms de domaines Internet. Il est possible de transformer par un algorithme tout nom de domaine Internet en un nom distinctif, et de reconvertir ces noms distinctifs en noms de domaines d'origine.

L'algorithme pour transformer un nom de domaine est de commencer par un nom distinctif (DN, *distinguished name*) et puis de rattacher des noms distinctifs relatifs (RDN, *Relative Distinguished Name*) pour chaque composant du domaine, avec le plus significatif (par exemple, le plus à droite) en premier. Chacun de ces RDN est un seul AttributeTypeAndValue *(type d'attribut et valeur)*, où le type est l'attribut "DC" et la valeur est une chaîne IA5 qui contient le composant du nom de domaine.

Donc, le nom de domaine "CS.UCL.AC.UK" peut être transformé en

DC=CS,DC=UCL,DC=AC,DC=UK

Les noms distinctifs dans lesquels il y a un ou plusieurs RDN, ne contenant tous que le type d'attribut DC, peuvent être retransposés en noms de domaines. Noter que le présent document ne définit pas une équivalence de nom de domaine pour d'autres noms distinctifs.

4. Définition de type d'attribut

Le type d'attribut DC (abrégé pour domainComponent) est défini comme suit :

(0.9.2342.19200300.100.1.25 NAME 'dc' EQUALITY caseIgnoreIA5Match
SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE)

La valeur de cet attribut est une chaîne qui contient un composant d'un nom de domaine. Le codage de IA5String à utiliser dans LDAP est simplement les caractères de la chaîne elle-même. La règle de confrontation pour égalité est insensible à la casse, comme dans le DNS actuel.

5. Définitions de classes d'objet

Un objet qui a un nom dérivé de son nom de domaine en utilisant l'algorithme de la section 3 est représenté comme une entrée dans le répertoire. L'attribut "DC" est présent dans l'entrée et utilisé comme le RDN.

Un attribut ne peut être présent que dans une entrée détenue par un serveur LDAP lorsque cet attribut est permis par la classe d'objet de l'entrée.

La présente section définit deux classes d'objet. La première, dcObject, est destinée à l'utilisation dans les entrées pour lesquelles il y a une classe d'objet structurelle appropriée. Par exemple, si le domaine représente une organisation particulière, l'entrée aurait comme classe d'objet structurelle "organisation", et la classe "dcObject" serait une classe auxiliaire. La seconde, "domain", est une classe d'objet structurelle utilisée pour des entrées dans lesquelles aucune autre information n'est mémorisée. La classe d'objet "domain" est normalement utilisée pour des entrées qui sont des fourre-tout ou dont les domaines ne correspondent pas à des entités du monde réel.

5.1 Classe d'objet "dcObject"

La classe d'objet dcObject permet que l'attribut dc soit présent dans une entrée. Cette classe d'objets est définie comme auxiliaire, car elle sera normalement utilisée en conjonction avec une classe d'objets structurelle existante, comme une organisation, une unité organisationnelle ou une localité.

La classe d'objet suivante, avec l'attribut dc, peut être ajoutée à toute entrée.

(1.3.6.1.4.1.1466.344 NAME 'dcObject' SUP top AUXILIARY MUST dc)

Un exemple d'entrée pourrait être :

```
dn: dc=critical-angle,dc=com
objectClass: top
objectClass: organization
objectClass: dcObject
dc: critical-angle
o: Critical Angle Inc.
```

5.2 Classe d'objet "domain"

Si l'entrée ne correspond pas à une organisation, une unité organisationnelle ou autre type d'objet pour lequel une classe d'objet a été définie, la classe d'objet "domain" peut alors être utilisée. La classe d'objet "domain" exige que l'attribut "DC" soit présent, et elle permet que plusieurs autres attributs soient présents dans l'entrée.

L'entrée aura pour classe d'objet structurelle la classe d'objet "domain".

```
( 0.9.2342.19200300.100.4.13 NAME 'domain' SUP top STRUCTURAL
 MUST dc
 MAY ( userPassword $ searchGuide $ seeAlso $ businessCategory $
 x121Address $ registeredAddress $ destinationIndicator $
 preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $
 telephoneNumber $ internationaliSDNNumber $ facsimileTelephoneNumber $
 street $ postOfficeBox $ postalCode $ postalAddress $
 physicalDeliveryOfficeName $ st $ l $ description $ o $
 associatedName ) )
```

Les attributs facultatifs de la classe "domain" sont utilisés pour décrire l'objet représenté par ce domaine, et peuvent aussi être utiles lors de recherches. Ces attributs sont déjà défnis dans l'utilisation de LDAP [4].

Un exemple d'entrée pourrait être :

```
dn: dc=tcp,dc=critical-angle,dc=com
objectClass: top
objectClass: domain
dc: tcp
description : entrée fourre-tout utilisée avec des enregistrements SRV
```

L'attribut DC est utilisé pour désigner des entrées de la classe "domain", et cela peut être représenté dans les serveurs X.500 par la règle de forme de nom suivante.

```
( 1.3.6.1.4.1.1466.345 NAME 'domainNameForm' OC domain MUST ( dc ) )
```

6. Références

[1] Recommandation UIT-T X.520, "L'annuaire : Types d'attributs choisis". 1993.

[2] P. Mockapetris, "Noms de domaines - Concepts et facilités", RFC1034, STD 13, novembre 1987.

[3] M. Wahl, S. Kille et T. Howes, "Protocole léger d'accès à un répertoire (LDAPv3) : Représentation de chaîne UTF-8 des noms distinctifs", RFC2253, décembre 1997.

[4] M. Wahl, "Résumé du schéma d'utilisateur X.500(96) à utiliser avec LDAPv3", RFC2256, décembre 1997. (*Obsolète, voir* RFC4517, RFC4519, RFC4523, RFC4512, RFC4510) *(P.S.)*

7. Considérations pour la sécurité

Le présent mémoire décrit comment les attributs des objets peuvent être découvert et restitués. Les serveurs devraient s'assurer qu'une politique de sécurité appropriée est respectée.

Une entreprise n'est pas limitée en ce qui concerne les informations qu'elle peut mémoriser dans des serveurs DNS ou LDAP.

Un client qui contacte un serveur qui n'est pas de confiance peut se voir retourner des informations incorrectes ou trompeuses (par exzmple, le serveur d'une organisation peut prétendre détenir des contextes de désignation représentant des noms de domaines qui n'ont pas été délégués à cette organisation).

8. Adresse des auteurs

Steve Kille
Isode Ltd.
The Dome
The Square

Richmond, Surrey
TW9 1DT
United Kingdom
téléphone : 181-332-9091
mél : S.Kille@ISODE.COM

Mark Wahl
Critical Angle Inc.
4815 W. Braker Lane #502-385
Austin, TX 78759

USA
téléphone : (1) 512 372 3160
mél : M.Wahl@critical-angle.com

Al Grimstad
AT&T
Room 1C-429,
101 Crawfords Corner Road
Holmdel, NJ 07733-3030
USA
mél : alg@att.com

Rick Huber
AT&T
Room 1B-433, 101 Crawfords Corner Road
Holmdel, NJ 07733-3030
USA
mél : rvh@att.com

Sri Sataluri
AT&T
Room 4G-202, 101 Crawfords Corner Road
Holmdel, NJ 07733-3030
USA
mél : sri@att.com

9. Déclaration complète de droits de reproduction