Groupe de travail sur les réseaux
Requête pour Commentaires : 2254
Catégorie : Standard
Traduction : Yves lescop

T. Howes
Netscape Communications Corp.
Décembre 1997
Lycée la croix-rouge - Brest

La représentation des filtres de recherche LDAP

1. Statut de ce document

Ce document spécifie un protocole standard d'Internet pour la communauté Internet, et ne sera éprouvé qu'après plusieurs discussions et suggestions. Merci de vous référer à l'édition courante du " Internet Official Protocol Standards " (STD1) pour l'état de standardisation et le statut de ce protocole. La distribution de ce document est illimitée.

Copyright

Note d'IESG

Ce document décrit un protocole d'accès à un annuaire qui fournit tant l'accès en lecture que l'accès pour mise à jour. L'accès de mise à jour exige une authentification sécurisée, mais ce document n'exige la mise en place d'aucun mécanisme d'authentification adéquat.

Selon RFC 2026, section 4.4.1, cette spécification est approuvé par IESG comme norme proposée en dépit de cette limitation, pour les raisons suivantes :

a. pour encourager la mise en place et le test d'interopérabilité de ces protocoles (avec ou sans l'accès de mise à jour) avant qu'ils soient déployés, et

b. pour encourager le déploiement et l'utilisation de ces protocoles dans des applications à lecture seule. (par exemple applications où LDAPv3 est utilisé comme langage d'interrogation pour les annuaires qui sont mis à jour par un mécanisme sécurisé autre que LDAP), et

c. pour éviter de retarder l'avancement et le déploiement d'autres protocoles standard d'Internet qui exigent la possibilité de questionner, mais pas de mettre à jour, des serveurs d'annuaire LDAPv3.

Les lecteurs sont avertis par la présente que jusqu'à ce que des mécanismes obligatoires d'authentification soient normalisés, les clients et les serveurs écrits selon cette spécification qui se servent de la fonctionnalité de mise à jour sont IMPROBABLEMENT INTEROPERABLE,

ou PEUVENT INTEROPERER SEULEMENT SI L'AUTHENTIFICATION EST RÉDUITE À UN NIVEAU INADMISSIBLEMENT FAIBLE.

Les implanteurs sont découragés par la présente de déployer des clients ou des serveurs LDAPv3 qui mettent en œuvre la fonctionnalité de mise à jour, jusqu'à ce qu'une norme proposée pour l'authentification obligatoire dans LDAPv3 ait été approuvée et éditée comme RFC.

2. Résumé

Le protocole LDAP ("Lightweight Directory Access Protocol") [1] définit une représentation en réseau d'un filtre de recherche transmis à un serveur LDAP. Quelques applications peuvent la trouver utile pour avoir une méthode générique de représenter ces filtres de recherche sous une forme lisible pour l'homme. Ce document définit un format de chaîne de caractères lisible pour l'homme pour représenter les filtres de recherche LDAP.

Ce document remplace le RFC 1960, étendant la définition de la chaîne de caractères de filtre LDAP pour inclure le support des filtres d'appariement étendus de la version 3 de LDAP, et incluant le support pour la représentation de la gamme complète des filtres de recherche possibles LDAP.

3. Définition de Filtre de Recherche LDAP

Un filtre de la recherche LDAPv3 est défini dans la section 4.5.1 [1] de comme suit :

```
Filter ::= CHOICE {
        and                [0] SET OF Filter,
        or                 [1] SET OF Filter,
        not                [2] Filter,
        equalityMatch      [3] AttributeValueAssertion,
        substrings         [4] SubstringFilter,
        greaterOrEqual     [5] AttributeValueAssertion,
        lessOrEqual        [6] AttributeValueAssertion,
        present            [7] AttributeDescription,
        approxMatch        [8] AttributeValueAssertion,
        extensibleMatch    [9] MatchingRuleAssertion
}

SubstringFilter ::= SEQUENCE {
        type    AttributeDescription,
        SEQUENCE OF CHOICE {
                initial        [0] LDAPString,
                any            [1] LDAPString,
                final          [2] LDAPString
        }
}

AttributeValueAssertion ::= SEQUENCE {
        attributeDesc   AttributeDescription,
        attributeValue  AttributeValue
```

```
}

MatchingRuleAssertion ::= SEQUENCE {
        matchingRule    [1] MatchingRuleID OPTIONAL,
        type            [2] AttributeDescription OPTIONAL,
        matchValue      [3] AssertionValue,
        dnAttributes    [4] BOOLEAN DEFAULT FALSE
}

AttributeDescription ::= LDAPString

AttributeValue ::= OCTET STRING

MatchingRuleID ::= LDAPString

AssertionValue ::= OCTET STRING

LDAPString ::= OCTET STRING
```

Le "LDAPString" ci-dessus est limité au codage UTF-8 du jeu de caractères ISO 10646 [4]. La "AttributeDescription" est une représentation en chaîne de caractères de la description d'attribut et est définie dans [1]. La CHAÎNE DE CARACTÈRES d'OCTET de "AttributeValue" et de "AssertionValue" ont la forme définie dans [2]. Le filtre est encodé pour la transmission sur un réseau en utilisant les règles encodantes de base définies dans [3], avec les simplifications décrites dans [1].

4. Définition de la Chaîne de caractères du Filtre de Recherche

La représentation en chaîne de caractères d'un filtre de recherche LDAP est définie par la grammaire suivante, suivant la notation ABNF définie dans [5]. Le format du filtre utilise une notation de préfixe.

```
filter     = "(" filtercomp ")"
filtercomp = and / or / not / item
and        = "&" filterlist
or         = "|" filterlist
not        = "!" filter
filterlist = 1*filter
item       = simple / present / substring / extensible
simple     = attr filtertype value
filtertype = equal / approx / greater / less
equal      = "="
approx     = "~="
greater    = ">="
less       = "<="
extensible = attr [":dn"] [":" matchingrule] ":=" value
                / [":dn"] ":" matchingrule ":=" value
present    = attr "=*"
substring  = attr "=" [initial] any [final]
initial    = value
```

```
any        = "*" *(value "*")
final      = value
attr       = AttributeDescription de la Section 4.1.5 de [1]
matchingrule = MatchingRuleId de la Section 4.1.9 de [1]
value      = AttributeValue de la Section 4.1.6 de [1]
```

L'attr, le "matchingrule", et les constructions de valeur sont comme décrit dans la section correspondante de [1] donnée ci-dessus.

Si une valeur contient un quelconque des caractères suivants

Caractère	valeur ASCII
*	0x2a
(	0x28
)	0x29
\	0x5c
NUL	0x00

le caractère doit être encodé comme caractère antislash '\' (ASCII 0x5c) suivi des deux chiffres hexadécimaux représentant la valeur ASCII du caractère encodé. La casse des deux chiffres hexadécimaux n'est pas significative.

Ce mécanisme d'échappement simple élimine les ambiguïtés d'analyse du filtre et permet à n'importe quel filtre qui peut être représenté dans LDAP d'être représenté comme chaîne de caractères terminée par un NUL. D'autres caractères sans compter ceux énumérés ci-dessus peuvent être échappés en utilisant ce mécanisme, par exemple, les caractères non imprimables.

Par exemple, le filtre contrôlant si l'attribut "cn" contient une valeur avec le caractère "*" à n'importe quelle position serait représenté comme "(cn=*\2a*)".

Notez que, bien que la sous-chaîne et les productions actuelles dans la grammaire ci-dessus puissent produire la construction "attr=*" , cette construction est employée pour seulement dénoter un filtre de présence.

5. Exemples

Cette section donne quelques exemples de filtre de recherche écrits en utilisant cette notation.

```
(cn=Babs Jensen)
(!(cn=Tim Howes))
(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))
(o=univ*of*mich*)
```

Les exemples suivants illustrent l'utilisation d'appariement extensible.

```
(cn:1.2.3.4.5:=Fred Flintstone)
(sn:dn:2.4.6.8.10:=Barney Rubble)
```

```
(o:dn:=Ace Industry)
(:dn:2.4.6.8.10:=Dino)
```

Le deuxième exemple illustre l'utilisation de la notation ":dn" pour indiquer que la règle d'appariement "2.4.6.8.10" devrait être utilisée en faisant les comparaisons, et que les attributs du nom distinctif d'une entrée devraient être considérés comme une partie de l'entrée lors de l'évaluation de l'appariement.

Le troisième exemple dénote un appariement d'égalité, sauf que des composants de DN devraient être considérés comme une partie de l'entrée en faisant l'appariement.

Le quatrième exemple est un filtre qui devrait être appliqué à n'importe quel attribut supportant la règle d'appariement donnée (puisque l'attr a été délaissé). Les attributs supportant la règle d'appariement contenue dans le DN devraient également être considérés.

Les exemples suivants illustrent l'utilisation du mécanisme d'échappement.

```
(o=Parens R Us \28for all your parenthetical needs\29)
(cn=*\2A*)
(filename=C:\5cMyFile)
(bin=\00\00\00\04)
(sn=Lu\c4\8di\c4\87)
```

Le premier exemple montre l'utilisation du mécanisme d'échappement pour représenter des caractères parenthèse. Le second montre comment représenter "*" dans une valeur, l'empêchant d'être interprété comme indicateur de sous-chaîne. Le troisième illustre l'échappement du caractère antislash.

Le quatrième exemple montre un filtre recherchant la valeur de quatre octets 0x00000004, illustrant l'utilisation du mécanisme d'échappement pour représenter des données arbitraires, y compris des caractères NUL.

L'exemple final illustre l'utilisation du mécanisme d'échappement pour représenter divers caractères non-ASCII UTF-8.

6. Considérations Sécuritaires

Cette note décrit une représentation en chaîne de caractères des filtres de recherche de LDAP. Tandis que la représentation elle-même n'a aucune implication de sécurité connue, les filtres de recherche de LDAP en ont. Ils sont interprétés par des serveurs LDAP pour choisir les entrées dont des données sont recherchées. Les serveurs LDAP devraient faire attention, pour protéger les données qu'ils mettent à jour, à l'accès non autorisé.

7. Références

[1] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[2] Wahl, M., Coulbeck, A., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[3] Specification of ASN.1 encoding rules: Basic, Canonical, and Distinguished Encoding Rules, ITU-T Recommendation X.690, 1994.

[4] Yergeau, F., "UTF-8, a transformation format of Unicode and ISO 10646", RFC 2044, October 1996.

[5] Crocker, D., "Standard for the Format of ARPA Internet Text Messages", STD 11, RFC 822, August 1982.

8. Adresse de l'auteur

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Road
Mountain View, CA 94043
USA

Phone: +1 415 937-3419
EMail: howes@netscape.com

9. Copyright intégral