Groupe de travail Réseau
Request for Comments : 2891
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

T. Howes, Loudcloud
M. Wahl, Sun Microsystems
A. Anantha, Microsoft
août 2000

Extension de commande LDAP pour le tri côté serveur des résultats de recherche

Résumé
Le présent document décrit deux extensions de commandes LDAPv3 pour le tri, côté serveur, des résultats de recherches. Ces commandes permettent à un client de spécifier le type d'attribut et des règles de correspondance qu'un serveur devrait utiliser lorsque il retourne les résultats d'une demande de recherche LDAP. Les commandes peuvent être utiles lorsque le client LDAP a des fonctionnalités limitées ou pour quelque autre raison ne peut pas trier les résultats mais a quand même besoin qu'ils soient triés. Les autres commandes permises sur les opérations de recherche ne sont pas définies dans cette extension.

Les commandes de tri permettent à un serveur de retourner un code de résultat pour le tri des résultats qui est indépendant du code de résultat retourné pour l'opération de recherche.

Les mots clés "DOIT", "DEVRAIT" et "PEUT" utilisés dans ce document sont à interpréter comme décrit dans la [RFC2119].

1. Commandes

1.1 Commande de demande

Cette commande est incluse dans le message searchRequest *(demande de recherche)* au titre du champ Commandes du message LDAP, comme défini au paragraphe 4.1.12 de la [RFC2251].

Le type de commande est réglé à "1.2.840.113556.1.4.473". La criticité PEUT être VRAI ou FAUX (où absent est aussi équivalent à FAUX) au choix du client. La valeur de commande est une CHAINE D'OCTET, dont la valeur est le codage BER d'une valeur de la SEQUENCE suivante :

```
SortKeyList ::= SEQUENCE DE SEQUENCE {
        attributeType   AttributeDescription,
        orderingRule    [0] MatchingRuleId FACULTATIF,
        reverseOrder    [1] BOOLÉEN DEFAUT FAUX }
```

La séquence SortKeyList *(liste de clés de tri)* est dans l'ordre de la plus forte à la plus faible préséance de clé de tri.

Le MatchingRuleId *(identifiant de règle de correspondance)* comme défini au paragraphe 4.1.9 de la [RFC2251], DEVRAIT être valide pour le type d attribut auquel il s'applique. Si il ne l'est pas, le serveur va retourner "Correspondance inappropriée".

Chaque type d'attribut ne devrait apparaître qu'une seule fois dans la liste des clés de tri. Si un type d'attribut est inclus plusieurs fois dans la liste des clés de tri, le serveur devrait retourner une erreur "unwillingToPerform" *(refus d'exécution)* dans le sortResult *(résultat de tri)*.

Si la règle d'ordre *(orderingRule)* est omise, l'ordre de la règle de correspondance *(MatchingRule)* définie pour être utilisée avec cet attribut DOIT être utilisé.

Toute mise en œuvre conforme de cette commande DOIT permettre une liste de clés de tri d'au moins une clé.

1.2 Commande Réponse

Cette commande est incluse dans le message searchResultDone *(recherche terminée)* au titre du champ Commandes du message LDAP, comme défini au paragraphe 4.1.12 de la [RFC2251].

Le type de commande est réglé à "1.2.840.113556.1.4.474". La criticité est FAUX (PEUT être absente). La valeur de commande est une CHAINE D'OCTETS dont la valeur est le codage BER d'une valeur de la SEQUENCE suivante :

```
SortResult ::= SEQUENCE {
  sortResult       ENUMERATED {
     réussite                        (0), -- les résultats sont triés
     erreur de fonctionnement        (1), -- échec interne du serveur
     limite de temps                 (3), -- limite de temps atteinte avant l'achèvement du tri
     authentification forte exigée   (8), -- refus de retourner les résultats tries via un protocole non sûr
     limite admin excédée            (11), -- trop d'entrées correspondantes à trier pour le serveur
     pas cet attribut                (16), -- type d'attribut non reconnu dans la clé de tri
     correspondance inappropriée     (18), -- règle de correspondance non reconnue ou inappropriée dans la clé de tri
     droits d'accès insuffisants     (50), -- refus de retourner les résultats du tri à ce client
     occupé                          (51), -- trop occupé pour ce traitement
     refus d'exécuter                (53), -- incapable de trier
     autre                           (80)
     },
 attributeType [0] AttributeDescription FACULTATIF }
```

2. Interaction client-serveur

La commande Demande de clé de tri *(sortKeyRequest)* spécifie un ou plusieurs types d'attribut et de règles de correspondance pour les résultats retournés par une demande de recherche. Le serveur DEVRAIT retourner tous les résultats de la demande de recherche dans l'ordre spécifié par les clés de tri. Si le champ Ordre inverse est réglé à VRAI, les entrées seront alors présentées dans l'ordre de tri inverse pour la clé spécifiée.

Six scénarios peuvent se produire par suite de la commande de tri incluse dans la demande de recherche :

1 Si le serveur ne prend pas en charge cette commande de tri et si le client a spécifié VRAI dans le champ Criticité de la commande, le serveur DOIT alors retourner Extension critique indisponible comme code de retour dans le message Recherche terminée *(searchResultDone)* et ne pas renvoyer d'autre résultat. Ce comportement est spécifié au paragraphe 4.1.12 de la [RFC2251].

2 Si le serveur ne prend pas en charge cette commande de tri et si le client a spécifié FAUX dans le champ Criticité de la commande, le serveur DOIT alors ignorer la commande de tri et traiter la demande de recherche comme si elle n'était pas présente. Ce comportement est spécifié au paragraphe 4.1.12 de la [RFC2251].

3 Si le serveur prend en charge cette commande de tri mais pour une raison quelconque ne peut pas trier les résultats de la recherche en utilisant les clés de tri spécifiées et si le client a spécifié VRAI dans le champ Criticité de la commande, le serveur DEVRAIT alors faire ce qui suit : retourner Extension critique indisponible comme code de retour dans le message Recherche terminée ; inclure la commande Réponse de clé de tri *(sortKeyResponseControl)* dans le message Recherche terminée *(searchResultDone)* et ne renvoyer aucune entrée de résultat de recherche.

4 Si le serveur prend en charge cette commande de tri mais pour une certaine raison ne peut pas trier le résultat de recherche en utilisant les clés de tri spécifiées et si le client a spécifié FAUX dans le champ Criticité de la commande, le serveur devrait retourner tous les résultats de la recherche non triés, et inclure la commande "sortKeyResponseControl" dans le message Recherche terminée.

5 Si le serveur prend en charge cette commande de tri et s'il peut trier les résultats de la recherche en utilisant les clés de tri spécifiées, il devrait alors inclure la commande sortKeyResponseControl dans le message Recherche effectuée avec un résultat de tri de réussite.

6 Si la demande de recherche a échoué pour une raison quelconque et/ou si il n'y a pas de message d'entrées de résultat de recherche retourné pour la réponse de recherche, le serveur DEVRAIT alors omettre la commande de réponse de clé de tri du message Recherche effectuée.

L'application client est assurée que les résultats sont triés dans l'ordre de la clé spécifiée si et seulement si le code de résultat dans la commande de réponse de clé de tri est réussite. Si le serveur omet la commande de réponse de clé de tri du message Recherche effectuée, le client DEVRAIT supposer que la commande de tri a été ignorée par le serveur.

La commande de réponse de clé de tri, si elle est incluse par le serveur dans le message Recherche effectuée, devrait avoir le résultat de tri réglé soit à réussite si les résultats on été triés conformément aux clés spécifiées dans la commande de réponse de clé de tri, soit réglé au code d'erreur approprié disant pourquoi il n'a pas pu trier les données (comme Pas cet attribut ou Correspondance inappropriée). Facultativement, le serveur PEUT régler le type d'attribut au premier type d'attribut spécifié dans la liste de clés de tri qui était erroné. Le client DEVRAIT ignorer le champ Type d'attribut si le résultat du tri est réussite.

Le serveur peut n'être pas capable de trier les résultats en utilisant les clés de tri spécifiées parce qu'il peut ne pas reconnaître un des types d'attribut, parce que la règle de correspondance associée à un type d'attribut n'est pas applicable, ou parce que aucun des attributs dans la réponse de recherche n'est de ces types. Les serveurs peuvent aussi restreindre le nombre de clés permises dans la commande, comme de ne prendre en charge qu'une seule clé.

Les serveurs qui repassent les demandes à d'autres serveurs LDAP devraient s'assurer que le serveur qui satisfait la demande du client a trié le résultat entier avant de renvoyer les résultats.

2.1 Comportement dans un environnement chaîné

Si un serveur reçoit une demande de tri, le client s'attend à recevoir un ensemble de résultats triés. Si un client soumet une demande de tri à un serveur qui retransmet la demande et obtient des entrées de plusieurs serveurs, et si le client a réglé la criticité de l'extension de tri à VRAI, le serveur DOIT fusionner les résultats de tri avant de les retourner au client ou DOIT retourner Refus d'exécuter *(unwillingToPerform)*.

2.2 Autres questions de tri

Une entrée qui satisfait aux critères de recherche peut manquer d'une ou plusieurs des clés de tri. Dans ce cas, l'entrée est considérée comme ayant une valeur de NUL pour cette clé. La présente norme considère NUL comme étant une valeur supérieure à toutes les autres valeurs valides pour cette clé. Par exemple, si une seule clé est spécifiée, les entrées qui satisfont le critère de recherche mais n'ont pas cette clé se placent après toutes les entrées qui ont cette clé. Si le fanion Ordre inverse est établi, et si une seule clé est spécifiée, les entrées qui satisfont au critère de recherche mais n'ont pas cette clé se placent AVANT toutes les entrées qui ont bien cette clé.

Si une clé de tri a des attributs multi-valeurs, et si une entrée se trouve avoir plusieurs valeurs pour cet attribut et si aucune autre commande qui affecte l'ordre de tri n'est présente, le serveur DEVRAIT alors utiliser la valeur moindre (conformément à la règle ORDERING pour cet attribut).

3. Interaction avec les autres commandes de recherche

Lorsque la commande sortKeyRequestControl est incluse avec la commande pagedResultsControl comme spécifié dans la [RFC2696], le serveur devrait alors envoyer les messages searchResultEntry triés conformément aux clés de tri appliquées à l'ensemble de résultats entier. Le serveur ne devrait pas simplement trier chaque page, car cela donnerait un résultat erroné au client.

La liste de clés de tri doit être présente sur chaque message Demande de recherche du résultat. Elle devrait aussi ne pas changer entre les demandes de recherche pour le même ensemble de résultats. Si le serveur a trié les données, il DEVRAIT alors renvoyer une commande sortKeyResponseControl sur chaque message Recherche effectuée pour chaque page. Cela va permettre aux clients de déterminer rapidement si l'ensemble de résultats est trié, plutôt que d'attendre de recevoir l'ensemble de résultats entier.

4. Considérations pour la sécurité

Les mises en œuvre et les administrateurs devraient être conscients que permettre le tri des résultats pourrait permettre la restitution d'un grand nombre d'enregistrements provenant d'un certain service de répertoires, sans considération des limites administratives établies sur le nombre maximum d'enregistrements à retourner.

Un client qui désire tirer tous les enregistrements d'un service de répertoires pourrait utiliser une combinaison de tri et de mise à jour de filtres de recherche pour restituer tous les enregistrements d'une base de données en petits ensembles de résultats, circonvenant ainsi les limites administratives.

Ce comportement peut être contré par l'utilisation judicieuse de permissions sur les entrées du répertoire par l'administrateur et par une mise en œuvre intelligente des limites administratives sur le nombre d'enregistrements fournis à un client.

5. Références

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

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

[RFC2696] C. Weider, A. Herron, A. Anantha, T. Howes, "Extension de commande LDAP pour manipulation de résultats à localisation simple", septembre 1999. *(Information)*

6. Adresse des auteurs

Anoop Anantha
Microsoft Corp.
1 Microsoft Way
Redmond, WA 98052
USA
téléphone : +1 425 882-8080
mél : anoopa@microsoft.com

Tim Howes
Loudcloud, Inc.
615 Tasman Dr.
Sunnyvale, CA 94089
USA
mél : howes@loudcloud.com

Mark Wahl
Sun Microsystems, Inc.
8911 Capital of Texas Hwy Suite 4140
Austin, TX 78759
USA
mél : Mark.Wahl@sun.com

7. Déclaration complète de droits de reproduction

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