draft-haripriya-dynamicgroup-02

Groupes dynamiques pour LDAPv3

Ce document décris les pré-requis, les sémantiques, les éléments du schéma, et les opérations nécessaires pour une fonctionnalité de groupe dynamique dans LDAP. Un groupe dynamique est définis ici comme un objet groupe avec une liste de dn qui est dynamiquement générée en utilisant un critère de recherche LDAP. La liste des membres dynamique peut ainsi être interrogée par une opération search ou compare, et peut également être utilisée pour trouver les groupes dont un objet est membre. Cette fonctionnalité élimine une grande quantité d'effort administratif pour maintenir l'appartenance à des groupes et les opérations basées sur les rôles dans une grande entreprise.

Le schéma décris dans ce document définis 2 classes d'objet : 'groupOfNames', et 'groupOfUniqueNames', qui maintiennent une liste statique de DN dans leur attribut member et uniqueMember, respectivement, et sont typiquement utilisés pour décrire un groupe d'objets pour diverses fonctions. Les groupes dynamique sont des groupes normaux, mais permettent de spécifier des critères à utiliser pour évaluer les membres. Cela peut également être un supplément aux groupes statiques dans LDAP pour fournir de la flexibilité.

Pré-requis

Les pré-requis suivants devraient être en place :

1. La création et l'administration des groupes dynamique devraient être fait en utilisant des opérations LDAP normales
2. Les applications doivent être capable d'utiliser les groupes dynamique de la même manière qu'avec les groupes statiques pour lister les membres et l'évaluation des membres
3. L'interrogation des membre d'un groupe dynamique devrait être fait en utilisant des opérations LDAP normales, et devraient être consistants.

Définition et sémantique du schéma

Les classes des groupes dynamique sont définis par le schéma suivant :

ObjectClasses

dynamicGroup Cette objet structurel est utilisé pour créer un objet de groupe dynamique. Il est dérivé de groupOfNames

dynamicGroupOfUniqueNames Cette objet structurel est utilisé pour créer un objet de groupe dynamique dont la liste des membres sont maintenus dans un attribut uniqueMember. Il est dérivé de groupOfUniqueNames

dynamicGroupAux Cette classe auxiliaire est utilisée pour convertir un objet existant en un groupe dynamique. Il est dérivé de groupOfNames

dynamicGroupOfUniqueNamesAux Cette classe auxiliaire est utilisée pour convertir un objet existant en un groupe dynamique de membres uniques. Il est dérivé de groupOfUniqueNames

Attributes

memberQueryURL Décris les membres de la liste une utilisant un LDAPURL

excludedMember Utilisé pour exclure les entrées d'un groupe dynamique.

member il est surchargé lorsqu'utilisé avec un groupe dynamique. Il est utilisé pour lister les membres statiques d'un groupe dynamique. Si la même entrée est listée dans les attributs member et excludedMember, cet attribut a précédence

uniqueMember fonctionne de manière similaire à member. Il a également précédence sur excludedMember

dgIdentity Pour fournir des résultat consistants en traitant les critères de recherche, le serveur doit utiliser une simple identité d'autorisation. Si l'autorisation de l'identité est liée, la liste des membres va varier. Cette identité peut servir pour effectuer la recherche.

format LDAPURL

la notation BNF est listée ici pour référence

```
ldapurl = scheme COLON SLASH SLASH [host [COLON port]] [SLASH dn [QUESTION [attributes] [QUESTION [scope]
[QUESTION [filter] [QUESTION extensions]]]]]
scheme = "ldap"
dn = distinguishedName
attributes = attrdesc *(COMMA attrdesc)
attrdesc = selector *(COMMA selector)
selector = attributeSelector
scope = "base" / "one" / "sub"
extensions = extension *(COMMA extension)
extension = [EXCLAMATION] extype [EQUALS exvalue]
extype = oid
exvalue = LDAPString
EXCLAMATION = %x21 ; exclamation mark ("!")
SLASH = %x2F ; forward slash ("/")
COLON = %x3A ; colon (":")
QUESTION = %x3F ; question mark ("?")
```

schéma

```
( <OID.TBD> NAME 'memberQueryURL' SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
( <OID.TBD> NAME 'excludedMember' SUP distinguishedName )
( 2.5.4.31 NAME 'member' SUP distinguishedName )
( 2.5.4.32 NAME 'uniqueMember' SUP distinguishedName )
( <OID.TBD> NAME 'identity' SUP distinguishedName SINGLE-VALUE )

( <OID.TBD> NAME 'dynamicGroup' SUP groupOfNames STRUCTURAL MAY (memberQueryURL $ excludedMember $ dgIdentity
))
( <OID.TBD> NAME 'dynamicGroupOfUniqueNames' SUP groupOfUniqueNames STRUCTURAL MAY (memberQueryURL $
excludedMember $ dgIdentity ))
( <OID.TBD> NAME 'dynamicGroupAux' SUP groupOfNames AUXILIARY MAY (memberQueryURL $ excludedMember $
dgIdentity ))
( <OID.TBD> NAME 'dynamicGroupOfUniqueNamesAux' SUP groupOfUniqueNames AUXILIARY MAY (memberQueryURL $
excludedMember $ dgIdentity ))
```

Extension x-chain

Une nouvelle extension est définie pour utilise memberQueryURL dans les groupes dynamiques, appelé 'x-chain'. Elle ne prend pas de valeur. Si présent, le serveur doit suivre toute référence de continuation de recherche sur d'autres serveurs lors de la recherche de membres.

Multiple valeurs

memberQueryURL peut avoir plusieurs valeurs, et dans ce cas, les membres du groupe dynamique sera l'union de ces membres calculés.

Condition des membres

Un objet O est un membre d'un groupe dynamique G si et seulement si :
((O is a value of the 'member' or 'uniqueMember' attribute of G)
OR
((O is selected by the membership criteria specified in the 'memberQueryURL' attribute values of G)
AND
(O is not listed in the 'excludedMember' attribute of G)))
Si un membre M d'un groupe dynamique G apparaît être un groupe dynamique ou statique, les membres statiques et dynamique de M ne devraient pas être considérés membre de G. M est un membre de G cependant. La dernière condition est imposée parce que :

- les membre évalués récursivement peuvent dégrader les performances du serveur
- Des boucles peuvent se produire dans des situations particulières
- L'affirmation des membres dynamique ne peut pas être optimisée si le membership récursif est permis.

dgIdentity - implication de sécurité

Parce que cet attribut donne indirectement, mais effectivement accès à tout le monde avec les opération read ou compare sur les attributs member ou uniqueMember avec les permissions suffisantes pour obtenir un résultat DN depuis memberQueryURL, les implémentation de serveur ne devraient pas autoriser de populer cet attribut avec le DN de n'importe quel objet qui n'est pas administré par l'identité faisant le changement de cet attribut.

Opérations sur les groupes dynamiques

Les opérations suivantes devraient exposer la fonctionnalité de groupe dynamique. Cet opérations ne nécessitent pas de changement dans l'annuaire, lorsque le sujet est un objet dynamique, et tous les membres du groupe, incluant les membres dynamiques, auront les mêmes permissions sur l'entrée cible.

Lire un objet dynamique

Quand les attributs member d'un groupe dynamique est listé par le client en utilisant une opération de recherche, les valeurs de member retournés devraient contenir les membres statiques et dynamiques. Cette fonctionnalité ne nécessite pas de changement au protocole, et les client n'ont pas à se préoccuper des groupes dynamiques pour exploiter cette fonctionnalité. Cette fonctionnalité est utile pour les client qui déterminent les accès privilégiés à une ressource par eux-même, en lisant les membres d'un objet groupe.

Par exemple : les client qui lisent l'attribut member d'un objet groupe dynamique et tentent de supprimer des valeurs qui sont dynamiquent peuvent reçevoir une erreur spécifiant qu'un telle valeur n'existe pas.

le groupe dynamique cn=dg1,o=myorg avec les attributs suivant :
member : cn=admin,o=myorg
excludedMember : cn=guest,ou=finance,o=myorg
excludedMember : cn=robin,ou=finance,o=myorg
memberQueryURL : ldap :///ou=finance,o=myorg ? ?sub ?(objectclass=organizationalPerson)
S'il y a 5 organizationalPerson sous ou=finance,o=myorg avec les noms commun bob, alice, john, robin, et guest, la sortie d'une recherche LDAP sur cn=dg1,o=myorg, avec l'attribut listé contenant 'member' sera la suivante :
dn : cn=dg1,o=myorg
member : cn=admin,o=myorg
member : cn=bob,ou=finance,o=myorg
member : cn=alice,ou=finance,o=myorg
member : cn=john,ou=finance,o=myorg

Fonctionnalité Is Member Of

L'opération de comparaison LDAP permet de découvrir si un DN est membre d'un groupe dynamique. De même, le serveur devrait produire des résultats consistants avec différentes identités d'autorisation lorsqu'il traite cette requête, tant que ces identités ont le même accès à l'attribut member ou uniqueMember. En utilisant les données de l'exemple plus haut, une comparaison dur cn=dg1,o=myorg, pour l'AVA member=cn=bob,ou=finance,o=myorg va résulter en une réponse compareTrue.

Membres statiques

Parce qu'un groupe dynamique surcharge la sémantique des attributs member et uniqueMember, un mécanisme est nécessaire pour récupérer les valeurs statiques trouvées dans ces attributs dans un but de gestion. Une nouvelle option d'attribut est définie, appelée 'x-static' qui devrait être spécifié uniquement avec les attributs member et uniqueMember.

Exemples

1. La valeur memberQueryURL spécifie le critère d'appartenance pour une entrée de groupe dynamique comme "toutes les entrée inetOrgPerson qui ont leur attribut title à manager, et sont sous ou=hr,o=myorg" :
memberQueryURL : ldap :///ou=hr,o=myorg ? ?sub ?(&(objectclass=inetorgperson)(title=manager)) ?x-chain
2. Cet valeur laisse l'utilisateur spécifier le critère d'appartenance pour une entrée de groupe dynamique comme "toutes les entrées sur le serveur local, qui a soit un compte unix ou appartient au département unix, et sous le conteneur engineering" :
memberQueryURL : ldap :///ou=eng,o=myorg ? ?sub ?(|(objectclass=posixaccount)(department=unix))
3. Ces valeurs laissent l'utilisateur spécifier le critère de membership comme "toutes les entrées inetOrgPerson sur le serveur local, soit sous ou=eng,o=myorg soit sous ou=support,o=myorg"
memberQueryURL : ldap :///ou=eng,o=myorg ? ?sub ?(objectclass=inetorgperson)
memberQueryURL : ldap :///ou=support,o=myorg ? ?sub ?(objectclass=inetorgperson)