動的グループを静的グループに自動反映

概要

工学研究科LDAPの動的グループ（ou=people配下）を静的なグループに反映する。

静的なグループに記述するLDAPフィルタで検索を行い、マッチしたエントリをそのグループエントリのuniqueMemberやownerに登録する。動的なグループに対して、適切なLDAPフィルタを登録することにより、静的なグループとして扱えるようになる。

このドキュメントは以下のサーバにおいて、動的グループ(LDAPフィルタ)として定義されたものを、静的なグループに自動で反映する処理について記述する。

- 対象サーバ
  ldap1.kogaku.kyoto-u.ac.jp
  ldap2.kogaku.kyoto-u.ac.jp

背景

所属組織などは動的なグループとして表されているが、各アプリで認証に使用する際、静的グループしか扱えない場合がある。これを解消するために、動的に定義されたグループを静的グループとして扱えるようにする必要がある。
この場合、認証に使用する空の静的グループを作成し、該当属性に認証範囲としたいエントリを検索するLDAPフィルタを記述する。このようにすると、このスクリプトによりLDAPフィルタの検索が実行され、静的グループのuniqueMemberまたはownerにエントリが自動登録される。

動作仕様

ldapに登録されたou=groups配下の各エントリのうち、LDAP検索・反映する必要のあるものには、特別なobjectClassを付与するものとする。このobjectClassが付与されたエントリに対し、uniqueMemberまたはowner属性への反映処理を行なう。付与されていないものについては反映処理を行なわない。
また、uniqueMemberとownerのいずれか一方、あるいは両方を処理対象とする指定が可能となるよう、objectClassも2つ用意する。

- 静的グループについて
  - 処理される静的グループのベースエントリ
    ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
  - 処理対象とするときに付与するobjectClass(uniqueMember用)
    objectClass: kyoto-uGroupOfFilteredUniqueMembers
  - 処理対象とするときに付与するobjectClass(owner用)
    objectClass: kyoto-uGroupOfFilteredOwners
  - LDAPフィルタを記述する属性(uniqueMember用)
    searchFilterForUniqueMember
  - LDAPフィルタを記述する属性(owner用)
    searchFilterForOwner
- 検索対象について
  - 検索される対象のベースエントリ
    ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp

サーバ設定

ldapのschema設定

/etc/openldap/schema/kyoto-uEduPerson.schemaを編集して、以下のattributeおよびobjectClassを追加する。

- attribute

```
attributetype ( feideAttribute:10
        NAME 'searchFilterForUniqueMember'
        DESC 'search Filter to register entries as UniqueMembers of a static group.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024} )

attributetype ( feideAttribute:11
        NAME 'searchFilterForOwner'
        DESC 'search Filter to register entries as Owners of a static group.'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{1024} )
```

- objectClass

```
objectclass ( feideObjClass:6
        NAME 'kyoto-uGroupOfFilteredUniqueMembers'
        SUP top
        AUXILIARY
        MAY ( searchFilterForUniqueMember ) )

objectclass ( feideObjClass:7
        NAME 'kyoto-uGroupOfFilteredOwners'
        SUP top
        AUXILIARY
        MAY ( searchFilterForOwner ) )
```

反映用ldapユーザ

静的グループを動的グループに自動反映と同様のユーザを使用する。

反映スクリプト作成

自動反映するスクリプトを使用する。静的グループを動的グループに自動反映での枠組みに組み込む。内容は dynflgroup.zipを参照。

- 反映スクリプト
  /home/ldap/flgroupとして作成する。反映処理自体を行なう。直接は呼び出さない。
- ldap更新チェックスクリプト
  /home/ldap/chk_modify_ldapを使用。
- 前回反映時刻保存ファイル
  dyngrp_date.txtを使用。

自動実行登録

静的グループを動的グループに自動反映の処理として呼び出されるため、新たな登録は不要。

実行例

以下、LDAPフィルタの反映例を示す。

- 静的グループ（cn=test,ou=groups...）を以下のように設定

```
dn: cn=test,ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
objectClass: groupOfUniqueNames
objectClass: kyoto-uGroupOfFilteredOwners
objectClass: kyoto-uGroupOfFilteredUniqueMembers
cn: test
uniqueMember: cn=foo,ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
uniqueMember: uid=bar,ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
owner: cn=foo,ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
owner: uid=bar,ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
searchFilterForUniqueMember: (LDAPフィルタ。省略)
searchFilterForOwner: (LDAPフィルタ。省略)
```

objectClassとして「kyoto-uGroupOfFilteredOwners」「kyoto-uGroupOfFilteredUniqueMembers」を持っているので、「uniqueMember」「owner」属性について、検索・反映処理が行われる。

- 反映後のエントリ（例）

```
dn: cn=test,ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
objectClass: groupOfUniqueNames
objectClass: kyoto-uGroupOfFilteredOwners
objectClass: kyoto-uGroupOfFilteredUniqueMembers
cn: test
uniqueMember: cn=foo,ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
uniqueMember: uid=bar,ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
uniqueMember: uid=mike,ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
owner: cn=foo,ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
owner: uid=pawl,ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
searchFilterForUniqueMember: (LDAPフィルタ。省略)
searchFilterForOwner: (LDAPフィルタ。省略)
```

- 注意
  - LDAPフィルタが複数定義されているとき
    すべてのフィルタを順に検索し、各結果の和（重複をのぞく）を登録する。
  - LDAPフィルタの属性が無いとき
    対応objectClassが指定されているにもかかわらず、LDAPフィルタの属性が存在しないときは、検索結果なしとなる。（以降は「検索結果なしの場合」を参照）
  - LDAPフィルタの内容が不正な時
    検索結果なしとなる。ただしLDAPフィルタの属性が複数ある場合、１つの検索結果が「検索結果なし」となっても他のLDAPフィルタの結果により全体として「検索結果なし」になるとは限らない。
  - 検索結果なしの場合
    owner属性の場合:owner属性を持たないエントリとなる。
    uniqueMember属性の場合:uniqueMemberとしてダミーエントリのdnが1つ登録される。(uniqueMemberは必須属性のため属性を持たないエントリにはできないため)
    ダミーエントリは「cn=dummy,ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp」

View Edit