TD3 et 4 M3104 Annuaires Unifiés (Découverte des annuaires LDAP)

Pouchoulon/Dubreuil/Bory

Novembre 2015

Ce TD a pour objet de découvrir les composantes d'un annuaire LDAP à l'aide du client LDAP Apache Directory Studio. Il sera le client graphique de référence durant M3104. Il permet de travailler à la fois avec les serveurs LDAP v3 Apache Directory Server et Openldap.Il a aussi pour objet de faire la réplication multi-maitre avec ADS.Ce TD a été préparé sur une Debian 8 Jessie. Utilisez une Vm avec cette version lors du TD.

1 Installation de Apache Directory Studio et Server

Attention : ApacheDS a besoin d'une JRE 1.7 faire un java -version afin de vérifier votre version de JRE.

1. Téléchargez et installez ApacheDS, ApacheStudio depuis Didex.
2. Quel est l'intérêt pour un annuaire d'être développé en Java ?

> **Solution :** Portabilité of course : ADS s'installe sur windows MacOS ou Linux mais aussi voir `http://directory.apache.org/apacheds/basic-ug/1.1-what-apacheds-is.html`

2 Création de votre premier Directory Server sous ADS

Vous allez créer votre premier Directory Server le fichier ldif du tutorial ApacheDS à `http://directory.apache.org/apacheds/basic-ug/resources/apache-ds-tutorial.ldif`.

1. Configurez votre première connexion. Le dn de l'entrée admin est "uid=admin,ou=system" et le mot de passe par défaut est "secret". Les ports d'écoute par défaut de ApacheDS sont 10389 ou 10636 (LDAPS).
2. Quel sont les ports d'écoutes standards d'un annuaire ?

> **Solution :** 389 et 636

3. En suivant `http://directory.apache.org/apacheds/basic-ug/1.4.3-adding-partition.html` ajoutez une partition o=sevenseas. Quel est l'intérêt d'une partition ? Activez l'accès anonyme. Pensez à redémarrez le serveur après la création de la partition.

> **Solution :** Les données dans deux partitions différentes ne se mélangent pas , on peut donc avoir sans risque plusieurs annuaires sur une seule instance d'ApacheDS

4. Importez le ldif apache-ds-tutorial.ldif dans le Directory Server "sevenSeas".
5. Quelles sont les méthodes d'authentification supportées par ApacheDS ?
6. Comment sont encryptés les mots de passe des capitaines de navire ?
7. D'après la documentation de ApacheDS, quelles sont les bonnes pratiques pour la sécurité des mots de passe ?

8. Qu'est ce que Kerberos ? A l'IUT qu'est ce qui pourrait servir de serveur Kerberos ?
9. Ajoutez une nouvelle entrée en suivant `http://directory.apache.org/apacheds/basic-ug/2.1.1-adding-entries.html`. Quelle type d'opération l'annuaire fait-il ? Supprimer l'entrée et refaite la même chose avec l'interface graphique en copiant une entrée. Fichier ldif de l'entrée :

```
# File captain_hook.ldif

dn : cn=James Hook,ou=people,o=sevenSeas
objectclass : inetOrgPerson
objectclass : organizationalPerson
objectclass : person
objectclass : top
cn : James Hook
description : A pirate captain and Peter Pan's nemesis
sn : Hook
mail : jhook@neverland
userpassword : peterPan
```

Solution :

10. Afficher les attributs opérationnels pour une entrée de ou=people. A quoi sert plus particulièrement l'entryDN ? Retrouvez pour cette entrée le parent à partir du contenu de l'attribut parentid et d'une recherche. Retrouvez toutes les entrées ayant cette entryUUID.

Solution : Voir `http://www.zytrax.com/books/ldap/apd/` pour quelques explications sur quelques attributs opérationnels. L'usage des timestamp est évident afin de savoir quand les entrées , les UUID aussi puisque toute entrée dans l'arbre doit être unique il faut bien un "unique identifier". L'entrydn voir `http://tools.ietf.org/id/draft-zeilenga-ldap-entrydn-02.txt`. Le dn n'est pas un attribut et ne permet donc pas de faire des recherches via un filtre ce qui n'est pas le cas avec l'entryDN.
Un recherche rapide avec le filtre et le parentid permet de retrouver l'entrée ou encore en saisissant l'entrée dans le navigateur LDAP. (entryUUID=69b8df28-5b6e-4441-b4ee-4eb76e109e8b)

3 Jouons avec les objectClasses , les attributs et les schémas

1. Quel est l'objectClass qui appartient à toutes les entrées dans l'annuaire ? A quoi sert-il ?

Solution : object class top. De cet object class dérive tous les autres objectclass.

2. Utilisez le navigateur de schéma :
   a) Retrouvez les pères de l'objectClass InetOrgPerson ?
   b) Quels sont les attributs obligatoires et facultatifs pour objectClass InetOrgPerson ?
   c) Quels sont les objectClasses qui utilise l'attribut uid ?
   d) Quelles sont pour cet attribut les règles de comparaison ?
3. Retrouvez ces informations en ligne de commande.

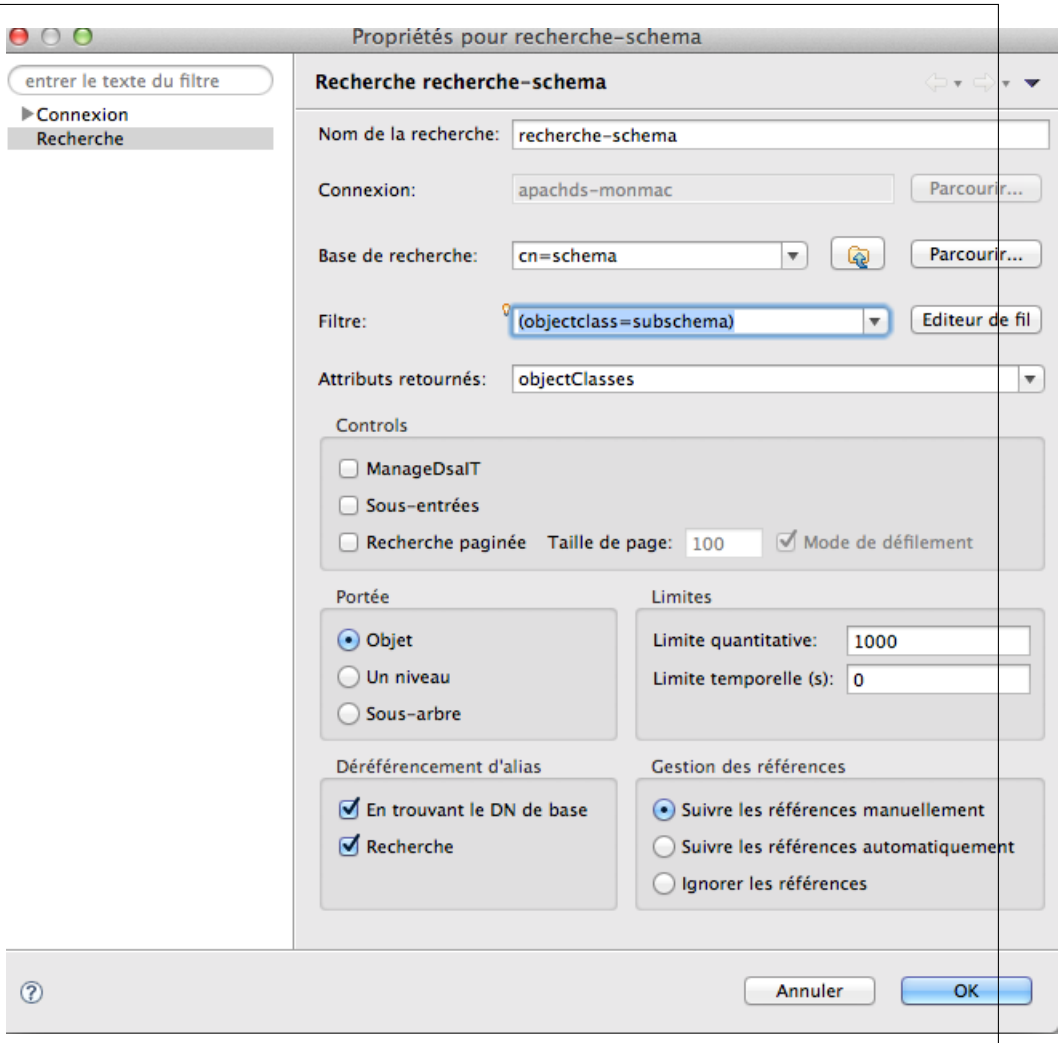
Solution :

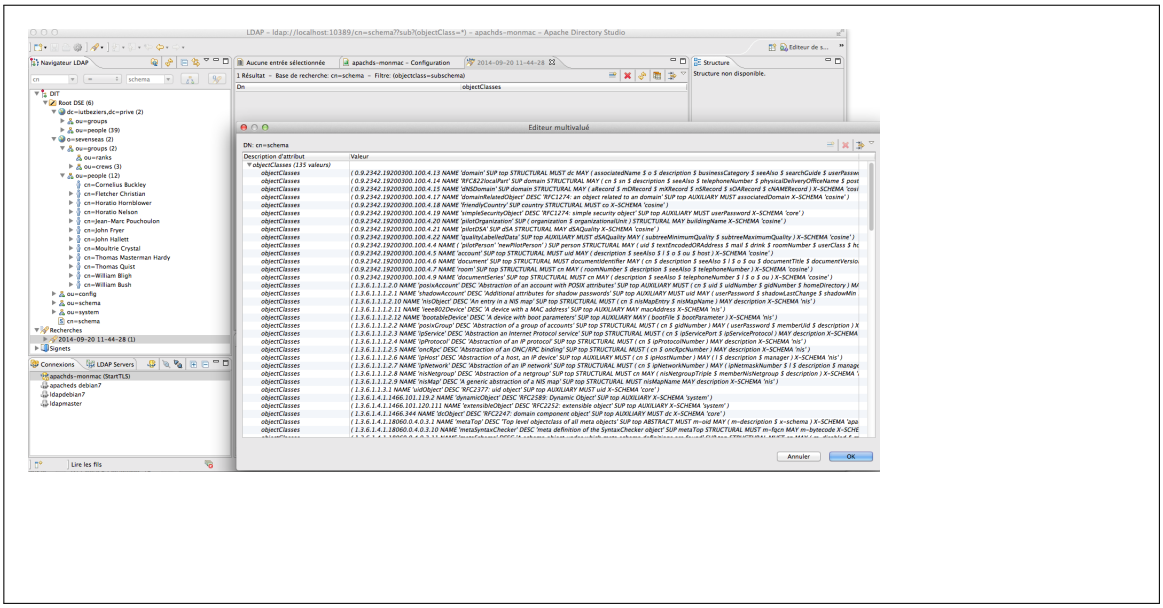
```
ldapsearch -h localhost -p 10389 -D "uid=admin,ou=system" -w ****** \
     -b "cn=schema" -s base "(objectclass=subschema)" objectclasses
...
objectClasses: ( 2.5.6.6 NAME 'person' DESC 'RFC2256: a person' SUP top
```

```
    STRUCTURAL MUST ( sn $ cn ) MAY ( userPassword $ telephoneNumber $
    seeAlso $ description ) X-SCHEMA 'core' )
...
ldapsearch -LLL -x -p 10389 -h localhost -D "uid=admin,ou=system" -w "secret" -b "ou=schema" "(
```

4. Refaite cette requête à l'aide de ApacheDS studio.

Solution :





5. Quels sont les schémas présents dans ApacheDS ?
6. On désire rajouter une ou=ships qui contiendra les navires comme décrit dans `http://directory.apache.org/apacheds/basic-ug/2.3.1-adding-schema-elements.html`. Cette manipulation étant complexe soyez concentré... Vous devez :
   — Ouvrir l'éditeur de schéma qui est différent de l'explorateur de schéma (en haut à droite de ApacheDS studio vous pouvez passez du browser LDAP à l'éditeur de schéma)
   — Créez un nouveau projet de schéma sevenSeas (Choisissez schéma en ligne).
   — Rajoutez l'attribut numberOfGuns en suivant la description ci-dessous puis ensuite l'ObjectClass ship en les saisissant.
   — Exportez le schéma dans un seul fichier ldif.
   — Revenez au browser LDAP et importez le fichier dans l'instance sevenSeas.
   — Importez les ldifs ci-dessous contenant l'ou=ships et l'entrée pour le HMS Victory.

```
attributetype ( 1.3.6.1.4.1.18060.0.4.3.2.1
        NAME 'numberOfGuns'
        DESC 'Number of guns of a ship'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
        SINGLE-VALUE
 )

objectclass ( 1.3.6.1.4.1.18060.0.4.3.3.1
        NAME 'ship'
        DESC 'An entry which represents a ship'
        SUP top
        STRUCTURAL
        MUST cn
        MAY ( numberOfGuns $ description )
 )
```

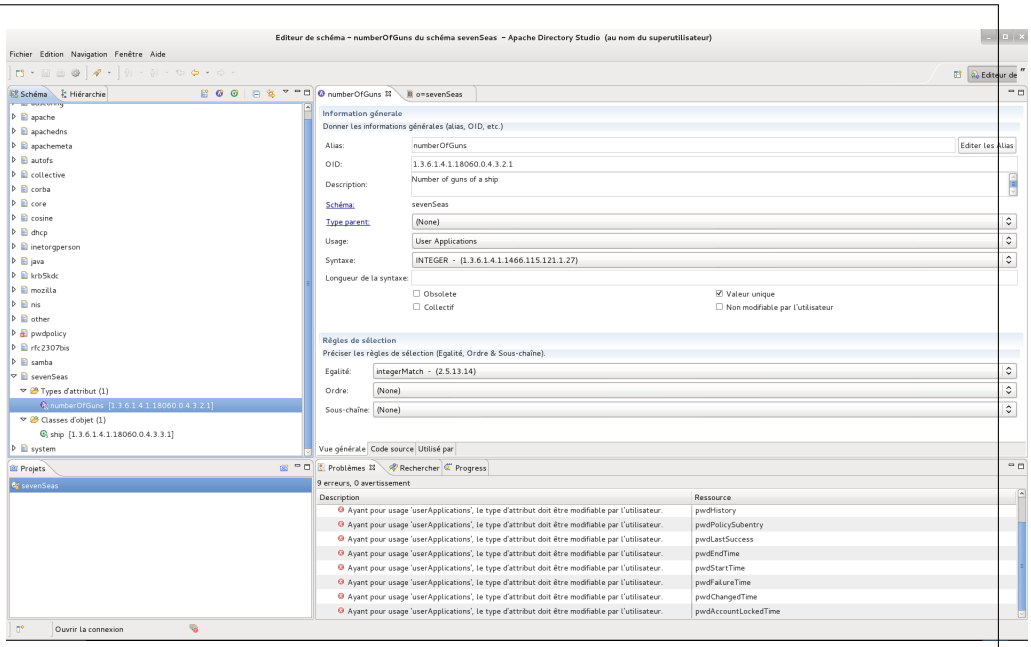
Le fichier ldif :

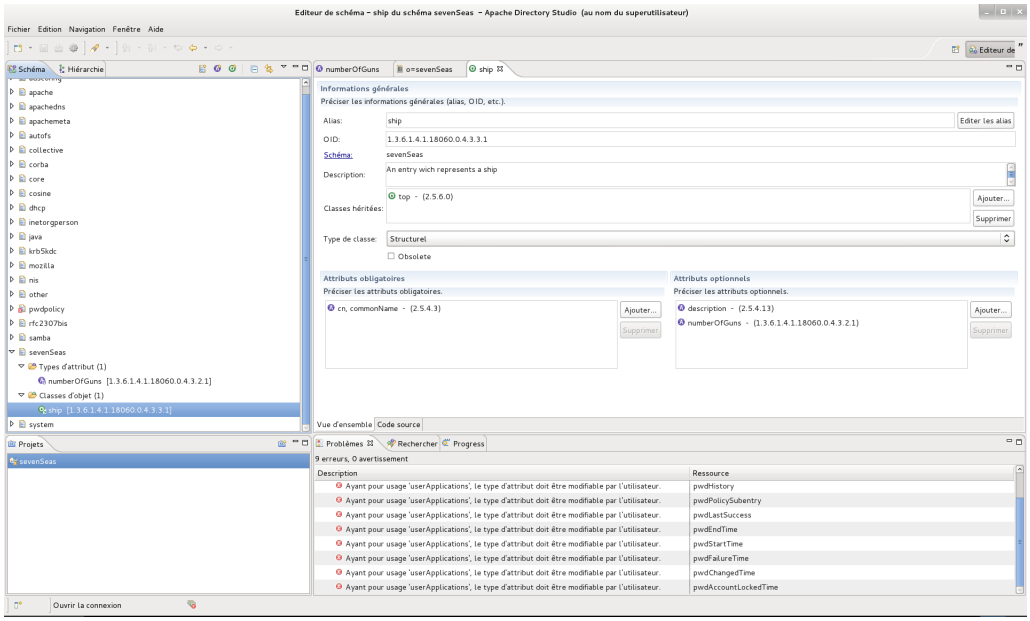
```
dn : ou=ships,ou=groups,o=sevenSeas
objectclass : organizationalUnit
objectclass : top
ou : ships
description : Contains entries which describe ships

dn : cn=HMS Victory,ou=ships,ou=groups,o=sevenSeas
```

```
objectClass : top
objectClass : ship
cn : HMS Victory
numberOfGuns : 104
description : a ship of the line of the Royal Navy
description : built between 1759 and 1765
```

Solution :

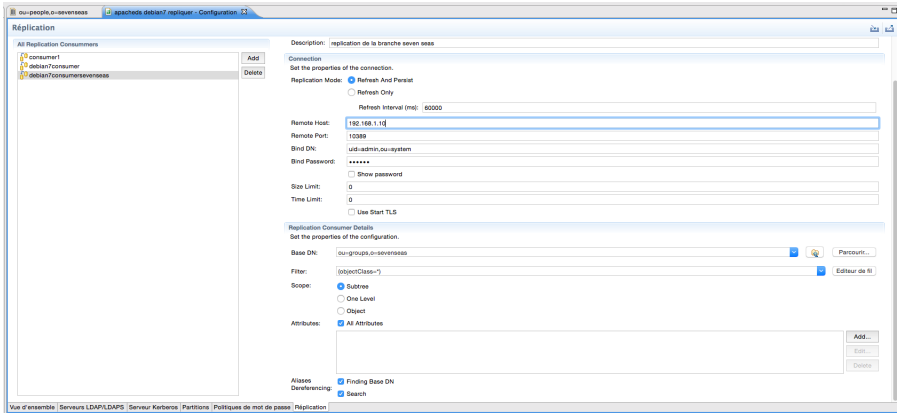




4 Réplication de ApacheDS

1. Configurer à l'aide de Apache Directory Studio la réplication de la branche people entre deux Apache Directory Server en mode multi-maitre.Vous pouvez vous aider de `http://joacim.breiler.com/apacheds/ch08s02.html`.

Solution :



5 Troubleshooting

— Attention si vous ne pouvez pas vous connecter sur le port 10389 vérifiez que le fichier pid soit vide.Voir /var/lib/apacheds<version>/default/run/*.pid.
— Les logs sont sous /var/lib/apacheds<version>/default/logs/
— Si nécessaire utilisez un sed -i afin d'enlever les M̂ présents dans le fichier apache-ds-tutorial.ldif (A quoi sert l'option -i ?) Pour faire un M̂ faire <Ctrl-V><Ctrl-M> au clavier.

```
# exécution in-place ( sed modifie le fichier avec -i)
sed -i s/^M//g apache-ds-tutorial.ldif
```