Atelier LDAP

La Plateforme en Ligne Mathrice (PLM) s'appuie sur un annuaire LDAP pour authentifier les utilisateurs sur les différents services proposés (revues en ligne, messagerie électronique).

L'objectif de cet atelier est que les laboratoires affiliés à Mathrice profitent de cette source d'authentification et l'utilisent sur des services de proximité (intranet, sessions interactives…). Ainsi les utilisateurs auront le même mot de passe qu'ils utilisent la PLM ou les services du laboratoire.

Pour y parvenir, nous vous proposons de mettre en oeuvre une réplique LDAP de l'annuaire de la PLM au sein de votre laboratoire.

---

start.txt · Dernière modification: 2013/10/01 08:32 par benoit

Atelier LDAP

Pré-requis

Voici les pré-requis nécessaires à la réalisation de cet atelier :

- une machine virtuelle (ou physique) au sein du système informatique de son laboratoire, elle est accessible à distance via SSH (directement ou à l'aide d'un serveur de rebond)
- la machine en question dispose d'un disque de 8Go et de 1Go de RAM
- installer une distribution GNU/Linux minimale (avec au moins SSH), de préférence une Debian 7 (utilisée pour les exemples)
- un ordinateur portable (équipé en WIFI et configuré pour Eduroam) à apporter avec soi le jour de l'atelier
- être un administrateur de branche pour la PLM. Concrètement, cela veut dire que vous devez avoir une icone “Gestion des comptes” dans l'interface webmail.math.cnrs.fr. Vous pouvez alors créer des comptes Mathrice à vos chercheurs.

Il est également nécessaire de vérifier que votre machine virtuelle, qui sera votre replica LDAP de laboratoire, puisse se connecter au serveur d'annuaire de la PLM. La commande openssl ci-dessous permet de le vérifier.

```
openssl s_client -connect auth.mathrice.fr:636
```

Pour le bon déroulement de l'atelier, chaque participant doit s'inscrire sur le sondage ci-dessous en précisant les pré-requis qu'il a pu valider.

https://ent.univ-poitiers.fr/studs/studs.php?sondage=4nosuqf1g8dgzk2z [https://ent.univ-poitiers.fr/studs/studs.php?sondage=4nosuqf1g8dgzk2z]

En complément, vous pouvez aussi (mais ce n'est pas obligatoire) :

- Créer un certificat X509 pour que votre réplique d'annuaire puisque parler en SSL avec vos clients. Pour cela, vous pouvez utiliser TERENA ou la PKI du CNRS. Si vous n'avez pas le temps de le faire, pas de problèmes, l'atelier inclus la création d'une certificat auto-signé.
- Pour vous faciliter la navigation LDAP (recherches), vous pouvez installer un client graphique LDAP sur l'ordinateur que vous utiliserez pendant l'atelier. L'outil Apache Directory Studio [http://directory.apache.org/studio/] est un bon candidat car il fonctionne sous les trois systèmes.

Retour

Atelier LDAP

Découverte de l'annuaire LDAP de la PLM

Organisation de l'annuaire

Comme tout annuaire LDAP, celui de la PLM possède une racine. Il s'agit de *dc=mathrice,dc=fr*. Il suit une organisation à plat avec plusieurs branches situées sous la racine dont :

- **o=People →** Les membres des laboratoires ; la notion d'appartenance à une unité de recherche est faite avec la valeur de l'attribut *ou*
- **o=Admin →** Les unités de recherche ; l'attribut *o* correspond à l'attribut *ou* de la branche o=People

```
dn: uid=metrot,o=people,dc=mathrice,dc=fr
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
objectClass: person
uid: metrot
gecos: Benoit Metrot
uidNumber: 2932
homeDirectory: /home/metrot
mailMathrice: Benoit.Metrot@math.cnrs.fr
loginShell: /bin/bash
sn: Metrot
ou: 6086
gidNumber: 2932
mail: benoit.metrot@math.univ-poitiers.fr

dn: cn=umr7348,o=admin,dc=mathrice,dc=fr
objectClass: groupOfUniqueNames
objectClass: top
uniqueMember: uid=metrot,o=People,dc=mathrice,dc=fr
description: Laboratoire de Mathematiques et Applications - Poitiers
o: 6086
cn: umr7348
```

Identifiant de laboratoire

Trouvez le numéro le numéro correspondant à votre laboratoire, en cherchant l'attribut ou de votre entrée dans l'annuaire. Remplacez <*login_plm*> par votre identifiant mathrice et <numero_unite> par le nombre contenu votre code unité.

```
ldapsearch -x -H ldaps://auth.mathrice.fr -D uid=<login_plm>,o=People,dc=mathrice,dc=fr -W -b o=Admin,dc=mathrice,dc=fr '(cn=*<numero_unite>
```

Dans le résultat de la recherche, répérez l'attribut o de l'entrée correspondant à votre unité. Notez le chiffre associé à cet entrée. Il correspondant à l'identifiant de votre unité au sein de l'annuaire. Ce numéro peut ne pas correspondre à le numéro actuel de votre unité.

Membres de votre unité

Avec la commande suivante, recherchez les membres de votre unité de recherche

```
ldapsearch -x -H ldaps://auth.mathrice.fr -D uid=<login_plm>,o=People,dc=mathrice,dc=fr -W -b o=People,dc=mathrice,dc=fr '(ou=<code_labo>)'
```

Retour

---

annuaireplm.txt · Dernière modification: 2013/10/01 08:36 par benoit

Atelier LDAP

Mise en oeuvre du replica local

Sur la machine virtuelle dédiée à la réplique d'annuaire, installez OpenLDAP à partir des paquets de la distribution. Pendant l'installation du paquet serveur OpenLDAP, saisissez un mot de passe non vide lorsqu'il le demande.

```
apt-get install slapd
```

Si vous n'avez pas saisi de mot de passe ou que vous voulez en changer, utilisez le fichier change-pw.ldif pour le remplacer. La commande *slappasswd* permet de générer le contenu du champ userPassword.

```
ldapmodify -QY EXTERNAL -H ldapi:/// -f change-rootpw.ldif
```

Avec slapcat, regarder les entrées générées au moment de l'installation du paquet

```
slapcat | grep '^dn:'
```

Supprimez les deux entrées ajoutées pendant l'installation du paquet slapd. Après avoir saisi tous les DN retournés par la commande précédente, tapez CTRL+D pour terminer la commande. Le mot de passe demandé est celui saisi lors de l'installation du paquet *slapd* (via DebConf).

```
ldapdelete -x -H ldap://127.0.0.1/ -D cn=admin,dc=prive -W
Password:
cn=admin,dc=prive
dc=prive
```

La racine définie dans la base LDAP n'est celle que nous voulons. Changez la en *dc=mathrice,dc=fr* avec le fichier change-root.ldif

```
ldapmodify -QY EXTERNAL -H ldapi:///  -f change-root.ldif
```

Insérez l'objet racine de l'arbre avec racine.ldif. Le mot de passe demandé est celui saisi pendant l'installation du paquet slapd.

```
ldapadd -x -H ldap://127.0.0.1/ -D cn=admin,dc=mathrice,dc=fr -W -f racine.ldif
```

Vérifiez le bon déroulement de l'ajout. Vous devriez voir apparaître l'entrée racine *dc=mathrice,dc=fr*.

```
ldapsearch -x -H ldap://127.0.0.1/ -b dc=mathrice,dc=fr
```

L'annuaire PLM a besoin d'attributs supplémentaires pour fonctionner. Ils ont été intégrés dans un schéma nis spécifique nis-mathrice.ldif. Pour l'installer, il est indispensable d'arrêter temporairement l'annuaire.

```
/etc/init.d/slapd stop
cd /etc/ldap/slapd.d/cn\=config/cn\=schema/
mv cn\=\{2\}nis.ldif /root
cp /root/nis-mathrice.ldif cn\=\{2\}nis-mathrice.ldif
tail -n 7 /root/cn\=\{2\}nis.ldif >> cn\=\{2\}nis-mathrice.ldif
/etc/init.d/slapd start
```

Il est également nécessaire d'élargir le schéma de l'annuaire afin de bénéficier d'attributs et de classes d'objet supplémentaires schema-lpk.ldif, schema-token.ldif, schema-samba.ldif, schema-qmail.ldif :

```
ldapadd -QY EXTERNAL -H ldapi:/// -f schema-lpk.ldif
ldapadd -QY EXTERNAL -H ldapi:/// -f schema-token.ldif
ldapadd -QY EXTERNAL -H ldapi:/// -f schema-samba.ldif
ldapadd -QY EXTERNAL -H ldapi:/// -f schema-qmail.ldif
```

Nous allons répliquer uniquement la branche contenant les comptes utilisateurs, soit o=People. Créez cette branche avec plm-branches.ldif.

```
ldapadd -x -H ldap://127.0.0.1 -D cn=admin,dc=mathrice,dc=fr -W -f plm-branches.ldif
```

Vérifiez le bon déroulement de l'ajout dans l'annuaire.

```
ldapsearch -x -H ldap://127.0.0.1/ -D "cn=admin,dc=mathrice,dc=fr" -W -b "o=People,dc=mathrice,dc=fr" '(ObjectClass=*)'
```

Si besoin, générez un certificat SSL autosigné, à l'aide de la commande OpenSSL :

```
cd /etc/ldap
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout slapd.key -out slapd.crt
```

Vous pouvez aussi utiliser des certificats CNRS2-Standard :

```
cp marepliqueplm.domain.key /etc/ldap/slapd.key
cp marepliqueplm.domain.pem /etc/ldap/slapd.pem
```

Veillez ensuite à bien positionner les droits d'accès sur les fichiers de certificat afin que le processus OpenLDAP puisse y accéder correctement.

```
cd /etc/ldap
chmod 644 slapd.crt
chown openldap.openldap slapd.key
chmod 600 slapd.key
```

Indiquez au serveur l'emplacement des certificats. Le fichier enable-tls.ldif augmente également le niveau de journalisation pour mieux observer ce qu'il se passe.

```
ldapmodify -QY EXTERNAL -H ldapi:/// -f enable-tls.ldif
```

La commande netstat vous montrera que le serveur OpenLDAP n'écoute pas encore en LDAPs mais seulement en LDAP (seulement une ligne en *:ldap LISTEN et pas en *:ldaps LISTEN

```
netstat -l --inet
```

Dans /etc/default/slapd, changer la ligne SLAPD_SERVICES comme suit de façon à autoriser uniquement les connexions SSL.

```
SLAPD_SERVICES="ldapi:/// ldaps:///"
```

Relancer le service d'annuaire. Vérifiez dans les logs (/var/log/syslog) et avec netstat que tout est opérationnel

```
/etc/init.d/slapd restart
```

A ce stade, vous pouvez configurer votre client graphique pour observer le contenu de votre réplique d'annuaire.

Enfin, il ne reste plus qu'à activer la replication LDAP depuis la machine de la PLM avec enable-syncrepl.ldif. Avant d'exécuter cette commande, modifiez ce fichier en remplaçant respectivement les X et les * par l'identifiant (*cn=….,o=replica,dc=mathrice,dc=fr*) et le mot de passe qui vous a été remis en début d'atelier.

Modifiez également le filtre de recherche, de façon à positionner la valeur de l'attribut *o* de votre unité repérée en début d'atelier. Par exemple, supposons que pour votre unité, l'attribut *o* a pour valeur 6086. Comme filtre LDAP, dans le fichier *enable-tls.ldif*, spécifiez *(&(objectClass=posixAccount)(ou=6086))*.

```
ldapadd -QY EXTERNAL -H ldapi:/// -f enable-syncrepl.ldif
```

Pour terminer, voici quelques points à vérifier pour que tout soit fonctionnel :

- Vérifier que la branche o=People est peuplée
- Vérifier que l'on peut s'authentifier sur la replique laboratoire avec son compte PLM (ldapsearch)
- Ajouter un compte dans l'interface Horde et regarder si elle apparait dans la réplique locale

Retour
