Modification de l'application Sésame

L'application Sésame de l'université doit être modifiée pour permettre :

- l'ajout des utilisateurs dans le royaume Kerberos lors de l'activation des comptes
- la modification du mot de passe des utilisateurs dans le royaume Kerberos (en plus de celle dans l'annuaire LDAP)
- la suppression des utilisateurs dans le royaume Kerberos lors de la suppression des comptes

Cela nécessite le branchement dans l'application, au même niveau que les actions effectuées sur l'annuaire LDAP et l'Active Directory, de l'appel des procédures équivalentes pour la maintenance de la cohésion du Royaume Kerberos avec la base des utilisateurs du S.II.

La mise à jour du royaume se fait en utilisant la commande **kadmin**, qui permet d'interagir avec la base de données de kerberos. **kadmin** n'offrant pas d'API, l'appel se fait à l'aide d'un appel système, de la même manière que décrit dans Installation du serveur CAS.

Configuration de Kerberos

En premier lieu, déclarer le *principal* qui servira à la mise à jour du royaume Kerberos (ici **sesame/admin**) et l'exporter dans le fichier **/etc/sesame-admin.keytab** :

```
[root@sesame ~]# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc -randkey sesame/admin
WARNING: no policy specified for sesame/admin@UNIV-RENNES1.FR; defaulting to no policy
Principal "sesame/admin@UNIV-RENNES1.FR" created.
kadmin:  ktadd -k /etc/sesame-admin.keytab sesame/admin
Entry for principal sesame/admin with kvno 3, encryption type Triple DES cbc mode with HMAC/sha1 added to
keytab WRFILE:/etc/cas-admin.keytab.
Entry for principal sesame/admin with kvno 3, encryption type ArcFour with HMAC/md5 added to keytab WRFILE:/etc
/cas-admin.keytab.
Entry for principal sesame/admin with kvno 3, encryption type DES with HMAC/sha1 added to keytab WRFILE:/etc
/cas-admin.keytab.
Entry for principal sesame/admin with kvno 3, encryption type DES cbc mode with RSA-MD5 added to keytab WRFILE:
/etc/cas-admin.keytab.
kadmin:  exit
[root@sesame ~]#
```

Le fichier **sesame-admin.keytab** doit être lisible par l'utilisateur **tomcat** :

```
[root@sesame ~]# cd /etc
[root@sesame etc]# chown root:tomcat sesame-admin.keytab
[root@sesame etc]# chmod 640 sesame-admin.keytab
[root@sesame etc]#
```

Il est également nécessaire de modifier les permissions du fichier de *log* de **kadmin** sans quoi l'appel de **kadmin** par l'utilisateur **tomcat** provoquerait une erreur.

```
[root@sesame ~]# cd /var/log
[root@sesame log]# touch kadmind.log
[root@sesame log]# chown root:tomcat kadmind.log
[root@sesame log]# chmod 664 kadmind.log
[root@sesame log]#
```

Exécution des requêtes kadmin

L'exécution d'une requête **kadmin** se fait de la manière suivante :

```
/usr/kerberos/sbin/kadmin -r UNIV-RENNES1.FR -p sesame/admin -k -t /etc/sesame-admin.keytab -q <query>
```

Pour ajouter un utilisateur dans le royaume, on utilisera la requête (**password** est le mot de passe de l'utilisateur, **uid** son identifiant) :

```
add_principal -pw password uid
```

Pour modifier le mot de passe d'un utilisateur dans le royaume, on utilisera la requête :

```
change_password -pw password uid
```

Enfin pour supprimer un utilisateur du royaume, on utilisera la requête :

```
delete_principal -force uid
```