Intégration d'un client Linux

Authentification

Configurer l'authentification des utilisateurs avec **system-config-authentication** :

- User information : Enable LDAP support, LDAP search base DN : **ou=people,dc=univ-rennes1,dc=fr**, LDAP server : **ldap://ldapglobal.univ-rennes1.fr**
- Authentication : Enable Kerberos support, Realm : **UNIV-RENNES1.FR**, KDCs : **kerb1.univ-rennes1.fr:88**, Admin servers : **kerb1.univ-rennes1.fr:749**
- sur les gentoo de l'IFSIC : il faut installer les paquets **mit-krb5** et **pam_krb5** et au final le fichier **/etc/pam.d/system-auth** doit avoir l'allure suivante :

```
auth       required     pam_env.so
auth       sufficient   pam_unix.so likeauth nullok
auth       sufficient   pam_krb5.so try_first_pass
auth       required     pam_deny.so

account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_krb5.so
account     required      pam_permit.so

password   required        pam_cracklib.so difok=2 minlen=8 dcredit=2 ocredit=2 retry=3
password   sufficient        pam_unix.so nullok md5 shadow use_authtok
password   required        pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_krb5.so
```

Configuration Kerberos

Vérifier le fichier **/etc/krb5.conf** :

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = UNIV-RENNES1.FR
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 UNIV-RENNES1.FR = {
  kdc = kerb1.univ-rennes1.fr:88
  kdc = kerb2.univ-rennes1.fr:88
  admin_server = kerb1.univ-rennes1.fr:749
  default_domain = univ-rennes1.fr
 }

[domain_realm]
 .univ-rennes1.fr = UNIV-RENNES1.FR
 univ-rennes1.fr = UNIV-RENNES1.FR

[appdefaults]
 pam = {
  debug = false
  ticket_lifetime = 36000
  renew_lifetime = 36000
  forwardable = true
  krb4_convert = false
 }
```

Créer le principal du client sous **kadmin** (depuis le client) et générer stocker la clé localement (dans **/etc/krb5.keytab**) :

```
[root@clinux log]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc -randkey host/clinux.ifsic.univ-rennes1.fr
WARNING: no policy specified for host/clinux.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "host/clinux.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  ktadd -k /etc/krb5.keytab host/clinux.ifsic.univ-rennes1.fr
Entry for principal host/clinux.ifsic.univ-rennes1.fr with kvno 3, encryption type AES-256 CTS mode with 96-bit
SHA-1 HMAC added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/clinux.ifsic.univ-rennes1.fr with kvno 3, encryption type AES-128 CTS mode with 96-bit
SHA-1 HMAC added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/clinux.ifsic.univ-rennes1.fr with kvno 3, encryption type Triple DES cbc mode with HMAC
/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/clinux.ifsic.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added
to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/clinux.ifsic.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/clinux.ifsic.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5
added to keytab WRFILE:/etc/krb5.keytab.
kadmin:  exit
[root@clinux log]#
```

Le shell des utilisateurs est renvoyé par l'attribut **loginShell** de l'annuaire LDAP. Si le shell des utilisateurs n'est pas installé, il faut alors l'installer (par exemple **yum install csh**).

Vérification de l'authentification des utilisateurs :

```
[root@clinux ~]# su - paubry
su: warning: cannot change directory to /private/staff/y/ry/paubry: No such file or directory
id: cannot find name for group ID 20857
su: /bin/csh: No such file or directory
[paubry@clinux ~]$ exit
logout
[root@clinux log]#
```

Monter les homedirs des utilisateurs en ajoutant dans **/etc/fstab** les lignes suivantes :

```
sf1ifsic:/vol/vol1/private/student /private/student nfs exec,nolock,dev,suid,rw,rsize=8192,wsize=8192 1 1
sf1ifsic:/vol/vol2/private/staff /private/staff nfs exec,nolock,dev,suid,rw,rsize=8192,wsize=8192 1 1
```

Créer puis monter les répertoires d'accueil :

```
[root@clinux ~]#
[root@clinux ~]# cd /
[root@clinux /]# mkdir -p /private/staff
[root@clinux /]# mkdir -p /private/student
[root@clinux /]# mount -a
[root@clinux /]# mount
[...]
sf1ifsic:/vol/vol1/private/student on /private/student type nfs (rw,nolock,rsize=8192,wsize=8192,addr=148.
60.4.42)
sf1ifsic:/vol/vol2/private/staff on /private/staff type nfs (rw,nolock,rsize=8192,wsize=8192,addr=148.60.4.42)
[root@clinux /]#
```

Ajouter si nécessaire le groupe des utilisateurs en local en ajoutant dans le fichier **/etc/group** :

```
staff:x:20857:
```

Enfin vérifier à nouveau le login des utilisateurs :

```
[root@clinux ~]# su - paubry
[paubry@clinux ~]$ exit
logout
[root@clinux ~]#
```

Configuration Firefox

Pour que l'authentification Kerberos soit propagée par Firefox, une petite configuration est nécessaire comme indiqué sur cette page : Configuration de Firefox pour le SSO.