Installation et configuration du serveur Kerberos (archive)

Installation système

Boot sur CD Fedora 10 puis upgrade vers Fedora 12.

- FQDN : kerb.ifsic.univ-rennes1.fr
- IP : 148.60.10.50

Packages additionnels installés :

- Servers -> Network servers -> kerb5-server

Configuration SELinux

Pour éviter de se prendre la tête lors de l'utilisation des utilitaires de configuration modifiant les fichiers système, on passe SELinux en mode permissif par la commande :

```
[root@kerb ~] setenforce 0
```

On peut aussi le faire pour les sessions suivantes (après reboot de la machine) en ajoutant la ligne :

```
SELINUX=disabled
```

dans le fichier **/etc/selinux/config** (ou bien simplement **SELINUX=permissive**).

Configuration Kerberos

Modification de quelques fichiers de configuration pour créer le royaume UNIV-RENNES1.FR.

/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
 default_etypes = des3-hmac-sha1 des-cbc-crc
 default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
 default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
 permitted_enctypes = des3-hmac-sha1 des-cbc-crc rc4-hmac
 ticket_lifetime = 24h
 forwardable = yes

[realms]
 UNIV-RENNES1.FR = {
  kdc = kerb.ifsic.univ-rennes1.fr:88
  admin_server = kerb.ifsic.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
 }
```

/var/kerberos/krb5kdc/kdc.conf

```
[kdcdefaults]
 v4_mode = nopreauth
 kdc_ports = 88,750
 kdc_tcp_ports = 88

[realms]
 UNIV-RENNES1.FR = {
  #master_key_type = aes256-cts
  acl_file = /var/kerberos/krb5kdc/kadm5.acl
  dict_file = /usr/share/dict/words
  admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
  supported_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-
sha1:normal des-cbc-md5:normal des-cbc-crc:normal des-cbc-crc:v4 des-cbc-crc:afs3 rc4-hmac:normal
 }
```

/var/kerberos/krb5kdc/kadm5.acl

```
*/admin@UNIV-RENNES1.FR        *
```

/etc/gssapi_mech.conf

En 64 bits seulement :

```
# library                              initialization function
# ===================================      =========================
# The MIT K5 gssapi library, use special function for initialization.
libgssapi_krb5.so                      mechglue_internal_krb5_init
```

Création de la base Kerberos :

```
[root@kerb ~]# kdb5_util create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'UNIV-RENNES1.FR',
master key name 'K/M@UNIV-RENNES1.FR'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
[root@kerb ~]#
```

Ajout du premier utilisateur (root) :

```
[root@kerb ~]# kadmin.local -q "addprinc root/admin"
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
WARNING: no policy specified for root/admin@UNIV-RENNES1.FR; defaulting to no policy
Enter password for principal "root/admin@UNIV-RENNES1.FR":
Re-enter password for principal "root/admin@UNIV-RENNES1.FR":
Principal "root/admin@UNIV-RENNES1.FR" created.
[root@kerb ~]#
```

Démarrage des services :

```
[root@kerb ~]# chkconfig kadmin on
[root@kerb ~]# service kadmin start
Starting Kerberos 5 Admin Server:                          [  OK  ]
[root@kerb ~]# chkconfig krb5kdc on
[root@kerb ~]# service krb5kdc start
Starting Kerberos 5 KDC:                                   [  OK  ]
[root@kerb ~]#
```

Vérification en affichant la liste des *principals* :

```
[root@kerb ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  listprincs
K/M@UNIV-RENNES1.FR
kadmin/admin@UNIV-RENNES1.FR
kadmin/changepw@UNIV-RENNES1.FR
kadmin/history@UNIV-RENNES1.FR
kadmin/kerb.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR
krbtgt/UNIV-RENNES1.FR@UNIV-RENNES1.FR
root/admin@UNIV-RENNES1.FR
kadmin:  exit
[root@kerb ~]#
```

Si à cette étape **kadmin** affiche le message d'erreur **Cannot contact any KDC for requested realm while initializing kadmin interface**, cela signifie que le serveur ne se trouve pas lui-même comme KDC et il faut vérifier sa configuration réseau.

Ajout d'un principal pour le KDC lui-même (indispensable pour la réplication) :

```
[root@kerb ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc -randkey host/kerb.ifsic.univ-rennes1.fr
WARNING: no policy specified for host/kerb.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "host/kerb.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  exit
[root@kerb ~]#
```

Ajout d'un utilisateur (paubry) pour les tests :

```
[root@kerb ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc paubry
WARNING: no policy specified for paubry@UNIV-RENNES1.FR; defaulting to no policy
Enter password for principal "paubry@UNIV-RENNES1.FR":
Re-enter password for principal "paubry@UNIV-RENNES1.FR":
Principal "paubry@UNIV-RENNES1.FR" created.
kadmin:  exit
[root@kerb ~]#
```

Configuration Firewall

Exécuter system-config-firewall et ouvrir les ports entrants suivants :

- 88 (pour kinit)
- 749 (pour les changements de mot de passe)
- 750 (pour l'authentification)