

# Intégration d'un client Windows 7 (archive)

## Déclaration du client Kerberos

Sur le KDC, ajouter le principal correspondant au client :

```
[root@kerb ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin: addprinc -pw password -e des-cbc-crc:normal host/cwin7.ifsic.univ-rennes1.fr
WARNING: no policy specified for host/cwin7.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "host/cwin7.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin: exit
[root@kerb ~]#
```

## Configuration Kerberos

Executer **cmd.exe** en tant qu'administrateur :

```
c:\> ksetup /addkdc UNIV-RENNES1.FR kerb.ifsic.univ-rennes1.fr
c:\> ksetup /setmachpassword password
c:\> ksetup /setrealm UNIV-RENNES1.FR
```

Rebooter le client puis exécuter (toujours en tant qu'administrateur) :

```
c:\> ksetup /mapuser * guest
```



Nous n'avons pas fait :

```
c:\> ksetup /addkpasswd UNIV-RENNES1.FR kerb.ifsic.univ-rennes1.fr
```

qui semble permettre le changement des mots de passe depuis les clients puisque ce n'est pas désiré (procédure centralisée depuis une page web qui devrait à terme mettre à jour l'annuaire LDAP et la base Kerberos).

## Modification le chiffrement

### Chiffrements autorisés

Demarrer -> Panneau de configuration -> Système et sécurité -> Outils d'administration -> Stratégies de sécurité locale -> Stratégies locales -> Sécurité réseau : configurer les types de chiffrement autorisés pour Kerberos : DES\_CBC\_CRC et DES\_CBC\_MD5.

cf <http://technet.microsoft.com/en-us/library/dd560670%28WS.10%29.aspx>

NB : cela modifie la clé de registre suivante :

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\SupportedEncryptionTypes (et la positionne à 0x03).

### Chiffrement par défaut

Mettre la valeur 0x17 (23) dans la clé de registre HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters.

## Sur le serveur kerberos

Malgré les modifications indiquées ci-dessus, les paquets TGS-REP (réponse à une demande de TGS) ne sont pas compris par les postes Windows 7. Le TGS-REP est en effet chiffré en 3DES qui semble -t-il pose problème. Une modification du krb5.conf (sur le serveur kerberos) règle problème :

```
default_realm = UNIV-RENNES1.FR
default_etypes = des3-hmac-sha1 des-cbc-crc
default_tkt_etypes = des3-hmac-sha1 des-cbc-crc
default_tgs_etypes = des3-hmac-sha1 des-cbc-crc
#permitted_etypes = des3-hmac-sha1 des-cbc-crc rc4-hmac
permitted_etypes = des-cbc-crc rc4-hmac
ticket_lifetime = 24h
forwardable = yes
```

Reste à vérifier si d'autres types d'encodage peuvent être introduits, l'image ci-dessous montre les types d'encodage supportés par Windows :

