Mise en place d'un serveur Samba

Nous montrons dans cette partie comment configurer Samba pour authentifier les utilisateurs avec Kerberos.

Configuration de Samba

Editer **/etc/samba/smb.conf** comme suit :

```
[global]
   kerberos method = system keytab
   realm = UNIV-RENNES1.FR
   security = ADS
   log file = /var/log/samba/log.%m
   hosts allow = 148.60.10. 127.

[tmp]
   comment = Temporary file space
   path = /tmp
   read only = no
   public = yes
```

Configuration Kerberos

Il faut à la fois déclarer le client (host) et le service SMB (cifs) dans le royaume Kerberos :

```
[root@server ~]# kadmin
Authenticating as principal root/admin@UNIV-RENNES1.FR with password.
Password for root/admin@UNIV-RENNES1.FR:
kadmin:  addprinc -randkey host/server.ifsic.univ-rennes1.fr
WARNING: no policy specified for host/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "host/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  ktadd host/server.ifsic.univ-rennes1.fr
Entry for principal host/server.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/server.ifsic.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added
to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES cbc mode with RSA-MD5
added to keytab WRFILE:/etc/krb5.keytab.
kadmin:  addprinc -randkey cifs/server.ifsic.univ-rennes1.fr
WARNING: no policy specified for cifs/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR; defaulting to no policy
Principal "cifs/server.ifsic.univ-rennes1.fr@UNIV-RENNES1.FR" created.
kadmin:  ktadd cifs/server.ifsic.univ-rennes1.fr
Entry for principal cifs/server.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 cifs/server.ifsic.univ-rennes1.fr with kvno 3, encryption type ArcFour with HMAC/md5 added
to keytab WRFILE:/etc/krb5.keytab.
Entry for principal cifs/server.ifsic.univ-rennes1.fr with kvno 3, encryption type DES with HMAC/sha1 added to
keytab WRFILE:/etc/krb5.keytab.
Entry for principal cifs/server.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@server ~]#
```

Tests

Clients Windows

Connecter un lecteur réseau sur **\\server.ifsic.univ-rennes1.fr\tmp**.

Clients linux

mount -t cifs étant réservé à l'utilisateur root, on valide le passage de l'authentification Kerberos avec **smbclient** en utilisant l'option **-k** :

```
[paubry@clinux ~]$ smbclient //server.ifsic.univ-rennes1.fr/tmp -k
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.4.2-47.fc12]
smb: > ls
  .                                   D        0  Fri Jan 22 15:25:32 2010
  ..                                 DR        0  Fri Jan 15 15:15:44 2010
  [...]
                36048 blocks of size 2097152. 32054 blocks available
smb: > exit
[paubry@clinux ~]$
```