Configuration de CUPS pour Kerberos (archive)

Dans l'architecture de test, le serveur CUPS est installé sur la machine cas.ifsic.univ-rennes1.fr.

Configuration du serveur

Générer le principal **ipp/cas.ifrsic.univ-rennes1.fr** et le stocker dans **/etc/krb5.keytab** :

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

Exécuter la commande suivante pour mettre en place l'authentification Kerberos :

```
[root@cas ~]# cupsctl DefaultAuthType=Negotiate
[root@cas ~]#
```

x