Mise en place d'un serveur NFS (v4-Kerberos)

Nous montrons dans cette partie comment configurer NFS (v4) pour authentifier les utilisateurs avec Kerberos.

Les tests sont fait sur la machine cas.ifsic.univ-rennes1.fr, sur laquelle on installe le serveur NFS (v4 par défaut).

La dernière partie montre al configuration d'un filer NetApp.

Configuration du serveur

Editer le fichier de configuration qui donne le mapping des utilisateurs pour tous les services basés sur RPC, dont NFS (**/etc/idmapd.conf**) :

```
Domain = univ-rennes1.fr
Local-Realms = UNIV-RENNES1.FR
```

Ajouter un principal pour le service NFS (nfs/cas.ifsic.univ-rennes1.fr) et l'ajouter au fichier /etc/krb5.keytab.

Préciser dans le fichier **/etc/exports** les répertoires à exporter :

```
/tmp      gss/krb5(sync,rw,fsid=0,no_subtree_check,anonuid=65534,anongid=65534)
```

Editer le fichier **/etc/sysconfig/nfs** et indiquer que l'on veut utiliser un NFS sécurisé :

```
SECURE_NFS="yes"
```

(re)Démarrer les services NFS et rpcidmapd.

Configuration du client

Ajouter dans la keytab du client le principal de root pour pouvoir faire les montages NFS :

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

Activer le module **rpcsec_gss_krb5** dans le noyau si nécessaire :

```
[root@clinux ~]# lsmod| grep rpc
auth_rpcgss            31232  1 nfs
sunrpc                158428  9 nfs,lockd,nfs_acl,auth_rpcgss
[root@clinux ~]# modprobe rpcsec_gss_krb5
WARNING: All config files need .conf: /etc/modprobe.d/anaconda, it will be ignored in a future release.
[root@clinux ~]# lsmod| grep rpc
rpcsec_gss_krb5         8824  0
auth_rpcgss            31232  2 rpcsec_gss_krb5,nfs
sunrpc                158428  10 rpcsec_gss_krb5,nfs,lockd,nfs_acl,auth_rpcgss
[root@clinux ~]#
```

*Ajouter ici comment insérer le module à chaque redémarrage.

Editer le fichier **/etc/sysconfig/nfs** et indiquer que l'on veut utiliser un NFS sécurisé :

```
SECURE_NFS="yes"
```

Démarrer le démon **rpcgssd** :

```
[root@clinux ~]# /etc/init.d/rpcgssd status
rpc.gssd is stopped
[root@clinux ~]# chkconfig rpcgssd on
[root@clinux ~]# /etc/init.d/rpcgssd start
Starting RPC gssd: WARNING: All config files need .conf: /etc/modprobe.d/anaconda, it will be ignored in a
future release.
                                                           [  OK  ]
[root@clinux ~]# /etc/init.d/rpcgssd status
rpc.gssd (pid 29697) is running...
[root@clinux ~]#
```

Effectuer les mêmes modification de **/etc/idmapd.conf** que sur le serveur et redémarrer le démon rpcidmapd :

```
[root@clinux ~]# /etc/init.d/rpcidmapd restart
Stopping RPC idmapd:                                       [ OK ]
Starting RPC idmapd:                                       [ OK ]
[root@clinux ~]
```

Monter à la main les répertoires :

```
[root@clinux ~]# mount -t nfs4 -osec=krb5 cas.ifsic.univ-rennes1.fr:/ /mnt
[root@clinux ~]#
```

Pour un montage automatique des répertoires, modifiers le fichier **/etc/fstab** :

```
cas.ifsic.univ-rennes1.fr:/ /mnt nfs4 sec=krb5
```

Installation Gentoo

Installer le package **nfs-utils** avec l'option kerberos:

```
USE="kerberos" emerge nfs-utils
```

Configuration NFS v4 avec un filer NetApp

Créer le principal du service nfs (**nfs/netapp.univ-rennes1.fr**) en utilisant l'option **-e des_cbc_crc:normal** (le seul chiffrement compris par NetApp), l'exporter dans **Unix_krb5.keytab** (toujours avec l'option **-e des_cbc_crc:normal**), puis copier ce fichier dans la hiérarchie **/etc** du filer (après un montage NFS v3 par exemple ou un FTP).

Executer **nfs setup** sur le filer, en spécifiant que l'on s'appuie sur un KDC Unix.

Lors de l'ajout d'un partage, spécifier **krb5** dans le paramètre **SECURITY** (égal à **sys** par défaut).

Enfin, la récupération des identités des utilisateurs doit être configuré de la manière suivante :

```
ldap.base                     dc=univ-rennes1,dc=fr
ldap.base.passwd              ou=people,dc=univ-rennes1,dc=fr
ldap.enable                   on
ldap.minimum_bind_level       anonymous
ldap.port                     389
ldap.servers                  ldapglobal.univ-rennes1.fr
ldap.servers.preferred        ldapglobal.univ-rennes1.fr
ldap.usermap.attribute.unixaccount uid
ldap.usermap.attribute.windowsaccount uid
ldap.usermap.enable           on
```

Les principals **root/client.ifsic.univ-rennes1.fr** doivent également être créés (et exportés dans le **/etc/krb5.keytab** des clients) en utilisant l'option **-e des_cbc_crc:normal**.