Authentification Kerberos

Lilian VARRAZ

Introduction

Le but de cet article est de mettre en œuvre un environnement sécurisé pour un utilisateur particulier. En effet, nous allons ajouter une couche "sécurité" au-dessus de l'environnement AIX standard, afin de permettre à certains utilisateurs de pouvoir passer des commandes à distance (*Remote Commands*) avec un degré de sécurité plus élévé.

Création d'un utilisateur standard AIX avec authentification Kerberos

Création d'un utilisateur standard AIX

Avant toute chose, il est **impératif** de créer un "utilisateur standard AIX" commun à tous les systèmes RS/6000 de votre environnement SP (*Control Work Station*, CWS, comprise).

- Créer un "utilisateur standard AIX", que l'on va nommer ici "kerberos" (mais qui pourrait avoir un autre nom), avec un UID égal à 229 et appartenant au groupe "STAFF", avec la commande :

```
# /usr/bin/mkuser id=229 pgrp=staff home=/home/kerberos kerberos
```

- Vérifier que les permissions soient identiques sur tous le nœuds (CWS comprise) sur le répertoire "/home/kerberos".

Création d'un utilisateur Kerberos "kerb" (sur la Control Work Station)

- Renseigner les chemins suivants au niveau de la variable "**PATH**" :

  /usr/lpp/ssp/kerberos/bin
  /usr/lpp/ssp/kerberos/etc
  /usr/kerberos/bin
  /usr/kerberos/etc

- Créer l'utilisateur authentifié "Kerberos" :

```
[cws]:root:/ # kdb_edit

Opening database...

Enter Kerberos V4 master key:  <PASSWD>
Previous or default values are in [brackets];
hit <enter> to leave the same, or new value.

Principal name: kerb
Instance: user
<not found>, Create [yes] ? y
Principal: kerb, Instance: user, kdc_key_ver: 1
New Password: *******
Verifying, please re-enter
New Password: *******
Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2038-01-01 ] ?
Max ticket lifetime [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:<CTRL-D>

[cws]:root:/ #
```

- Vérifier la création de cet utilisateur :

```
[cws]:root:/ # lskp kerb.user

kerb.user   tkt-life: 30d       key-vers: 1  expires: 2038-01-01 05:59
```

- Créer un *Key File* pour cette instance "user"

```
[cws]:root:/ # cd /home/kerberos

[cws]:root:/home/kerberos # ext_srvtab -n user
Generating 'user-new-srvtab'....
```

```
[cws]:root:/home/kerberos #
[cws]:root:/home/kerberos # ls -al

total 7
drwxr-xr-x  2 kerberos       staff       512 Apr 09 10:22 .
drwxr-xr-x  16 bin           bin         512 Apr 09 10:16 ..
-rwxr-----  1 kerberos       staff       486 Apr 08 15:05 .profile
-rw-------  1 kerberos       staff       928 Apr 09 10:17 .sh_history
-rw-------  1 root           system      26   Apr 09 10:22 user-new-srvtab

[cws]:root:/home/kerberos # klist -file user-new-srvtab -srvtab

Server key file:   user-new-srvtab
Service         Instance        Realm      Key Version
-------------------------------------------------
kerb            user            CWS          1

[cws]:root:/home/kerberos # chown kerberos:staff /home/kerberos/user-new-srvtab
[cws]:root:/home/kerberos # ls -al /home/kerberos/user-new-srvtab

-rw-------  1 kerberos       staff       26 Apr 09 10:22 user-new-srvtab

[cws]:kerberos:/home/kerberos # export KRBTKFILE=/tmp/tkt229
```

où **tkt229** correspond à l'UID de l'utilisateur kerberos

Sinon le message suivant apparaît :

```
ksrvtgt:  2502-054 The KRBTKFILE environment variable was not set
prior to issuing this command.
```

```
[cws]:kerberos:/home/kerberos# /usr/bin/ksrvtgt kerb user \
/home/kerberos/user-new-srvtab

[cws]:kerberos:/home/kerberos # kinit kerb.user

Kerberos V4 Initialization for «kerb.user»
Password: ******
```

- Créer le fichier "**.klogin**" dans la *home directory* de l'utilisateur "kerberos" (cette opération est à faire sur tous les nœuds, CWS compris) :

  A l'aide de votre éditeur préféré, créer un fichier "***.klogin***" dans "**/home/kerberos**" qui contient les informations suivantes :

  ```
  <user>.<instance>@<REALM>
  ```

  où REALM correspond au nom de votre royaume *kerberos*.
  Exemple : `kerb.user@cws`

- Valider l'installation en utilisant les "*remote commands*" :

  ```
  [cws]:kerberos:/home/kerberos# dsh -w <node> date
  ```

Utilisation de la fonction “kerberos” dans les “scripts”

Pour utiliser cette fonction *kerberos* à l’intérieur d’un *script*, il suffit d’insérer les lignes suivantes au début et à la fin de chaque *script* selon l’exemple suivant :

```
# Début
orkb4=$KRBTKFILE
export KRBTKFILE=/tmp/tkt<UID>
/usr/bin/ksrvtgt kerb user /home/kerberos/key
if [[ $? -ne 0 ]] then
     print “Failed to Get Kerberos V4 Credentials”
     exit 1
fi

# Votre script
(utilisant des commandes “dsh”, “pcp” ou autres remote commands)
.....
# Fin de votre script

/bin/k4destroy 1>/dev/null
if [[ orkb4 != “” ]] then
KRBTKFILE=$orbk4
else
KRBTKFILE
fi
# Fin
```

Bibliographie

- *Parallel System Programm supports for AIX “Administration Guide”*
- *“How to Rebuild the Kerberos Database on an IBM RS/6000 SP Control Workstation”*
  http://techsupport.services.ibm.com/server/aix.techTips
- *Red Book* : **SG24-5374** *“RS/6000 SP Cluster : The Path to Universal Clustering”*
  http://www.redbooks.ibm.com