

Authentification Kerberos : centralisation

Christophe ROMAC

Lorsque l'environnement SP devient complexe et qu'il y a plusieurs stations de contrôle (CWS), la gestion des tickets Kerberos peut devenir lourde. Dans ce cas, il est possible de centraliser l'authentification Kerberos sur une seule CWS. Nous allons voir comment faire, par le biais d'un exemple. Toutefois, cet exemple est basé sur deux CWS ; s'il y a plus de deux CWS, il faudra reproduire la manipulation pour les autres CWS et les autres nœuds.

Authentification centralisée de Kerberos

Nomination

CWS serveur d'authentification :	cws_master
Royaume de "cws_master" :	CWSMASTER
CWS en devenir client :	cws_client
Nœud appartenant à "cws_client" :	node1_cl

Mise en œuvre

- ① Sur "cws_master" :
modifier le fichier "/etc/krb.realms" pour y inclure la définition de "cws_client" ainsi que ses nœuds ; ici : "node1_cl".

```
<cws_master># echo "cws_client CWSMASTER" >> /etc/krb.realms  
<cws_master># echo "node1_cl CWSMASTER" >> /etc/krb.realms
```

Trucs et Astuces

- ② Depuis “cws_master”, il faut ensuite **propager les fichiers** “krb.realms” et “krb.conf” sur “cws_client” et “node1_cl”.

```
<cws_master># ftp cws_client
<cws_master>FTP > bin
<cws_master>FTP > put /etc/krb.realms /etc/krb.realms
<cws_master>FTP > put /etc/krb.conf /etc/krb.conf
```

Faire de même vers “node1_cl”.

- ③ Sur “cws_client” et “node1_cl” il faut alors **modifier le royaume** pour qu’il pointe sur le royaume de “cws_master”.

```
<cws_client># vi /.klogin
====> modifier tous les royaumes pour : @CWSMaster
```

Faire de même vers “node1_cl”.

- ④ Sur “cws_client” on peut maintenant **reconfigurer Kerberos**.

```
<cws_client># /usr/lpp/ssp/bin/setup_authent
```

- ⑤ Il reste maintenant à **régénérer** les clefs d’authentification sur les nœuds de “cws_client”.

```
<cws_master># /usr/lpp/ssp/kerberos/etc/ext_srvtab -n <if1_node1_cl> .... SPbgAdm
<cws_master># cat <if1_node1_cl>-new-srvtab .... SPbgAdm-new-srvtab > node1_cl-srvtab
```

Remarque : Sur toutes les interfaces que l’on désire authentifier sur le mode “Kerberos”, il faut **démultiplier** la première interface du nœud (if1_node1_cl).

- ⑥ Pour finir, il faut **transférer** cette nouvelle clef sur le nœud en question.

```
<cws_master># ftp node1_cl
<cws_master>FTP > bin
<cws_master>FTP > put node1_cl-srvtab /etc/krb-srvtab
```

- ⑦ Il faut enfin **activer** la nouvelle **clef Kerberos** .

```
<node1_cl># /usr/bin/k4init root.admin
```

- ⑧ On peut alors **valider** la nouvelle configuration de **Kerberos**.

```
<cws_client># s1term node1_cl  
====> ceci devrait fonctionner...
```

