Lab 4 : Mise en place de Kerberos

Dans ce tutoriel, nous allons vous montrer comment configurer l'authentification Kerberos entre deux serveurs Ubuntu 18.04.x. Nous allons installer et configurer le serveur Kerberos sur le serveur Ubuntu, puis installer le client Kerberos sur un autre machine Ubuntu.

1. Spécifications

- Serveur et client Ubuntu avec un utilisateur non-root avec des privilèges sudo.

Dans cet exemple:

	Adresse IP	FQDN
serveur	192.168.1.212	kdc.local.com
client	192.168.1.186	client.local.com

2. Configuration du FQDN sur le serveur et le client

- Serveur:

```
$ echo "192.168.1.212 kdc.local.com ctx12vm" | sudo tee -a /etc/hosts
$ sudo hostnamectl set-hostname kdc.local.com
```

- Client:

```
$ echo "192.168.1.186 client.local.com ctx06vm" | sudo tee -a /etc/hosts
$ sudo hostnamectl set-hostname client.local.com
```

3. Installation et configuration de seveur KDC Kerberos

```
$ sudo apt install -y krb5-kdc krb5-admin-server krb5-config
```

Au cours de l'installation, des questions seront posées sur le domaine Kerberos, le serveur Kerberos du domaine et le serveur administratif. Par défaut, le Kerberos utilisera le nom de domaine du serveur Kerberos comme REALM.

Dans notre cas:

- *Kerberos realm* - **local.lnxorg**
- *Kerberos server* - **kdc.local.com**
- *Administrative server* - **kdc.local.com**

Définition du mot de passe principal pour le REALM Kerberos :

```
$ sudo krb5_newrealm
```

Je dois créer l'utilisateur administrateur pour le serveur Kerberos du KDC (dans mon cas, le nom de l'administrateur est root), ajouter le nom d'hôte du serveur Kerberos à la base de données, puis créer la keytab pour le serveur Kerberos.

```
$ sudo kadmin.local
Authenticating as principal root/admin@LOCAL.LNXORG with password.

kadmin.local:  addprinc root/admin
WARNING: no policy specified for root/admin@LOCAL.LNXORG; defaulting to no
policy
Enter password for principal "root/admin@LOCAL.LNXORG":
Re-enter password for principal "root/admin@LOCAL.LNXORG":
Principal "root/admin@LOCAL.LNXORG" created.

kadmin.local:  addprinc -randkey host/kdc.local.com
WARNING: no policy specified for host/kdc.local.com@LOCAL.LNXORG;
defaulting to no policy
Principal "host/kdc.local.com@LOCAL.LNXORG" created.

kadmin.local:  ktadd host/kdc.local.com
Entry for principal host/kdc.local.com with kvno 2, encryption type aes256-
cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/kdc.local.com with kvno 2, encryption type aes128-
cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.

kadmin.local: quit
```

Nous devons ajouter le principe root/admin à la liste de contrôle d'accès en éditant le fichier /etc/krb5kdc/kadm5.acl et redémarrer le service.

```
$ echo "root/admin *" | sudo tee -a /etc/krb5kdc/kadm5.acl
sudo systemctl restart krb5-admin-server.service
sudo systemctl status krb5-admin-server.service
```

4. Installation et configuration client Kerberos

```
sudo apt install -y krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

Au cours de l'installation, des questions seront posées sur le Realm Kerberos, le serveur Kerberos du Realm et le serveur administratif. Les réponses sont les mêmes que pour l'installation du serveur.

Nous nous connectons au serveur Kerberos du KDC en utilisant la commande kadmin et le mot de passe pour le principe root/admin. Je dois ajouter le FQDN du client à la base de données Kerberos et au fichier keytab du client.

```
$ sudo kadmin
addprinc -randkey host/client.local.com
ktadd host/client.local.com
quit
```

5. Tests

Nous allons configurer l'authentification SSH en utilisant le protocole Kerberos. La machine cliente se connectera au serveur Kerberos via SSH avec l'authentification Kerberos.

5.1 Setup Serveur

Ajoute un nouvel utilisateur système nommé sshclient :

```
$ sudo useradd -m -s /bin/bash sshclient
```

Ajoute le même utilisateur à partir du niveau **kadmin** :

```
$ sudo kadmin.local
addprinc sshclient
quit
```

Nous devons activer l'authentification GSSAPIA dans la configuration ssh :

```
...
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
...
```

Redémarrage du service ssh :

```
$ sudo systemctl restart sshd.service
$ sudo systemctl status sshd.service
```

5.2 Setup Client

Ajoute un nouvel utilisateur système appelé *sshclien*t et se connecte au système :

```
$ sudo useradd -m -s /bin/bash sshclient
$ su - sshclient
```

Initialisation du principal utilisateur Kerberos *sshclient* :

```
kinit sshclient
```

Nous vérifions le billet disponible :

```
sshclient@ctx06vm:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1001_rw7I86
Default principal: sshclient@LOCAL.LNXORG

Valid starting       Expires              Service principal
18.03.2019 23:43:27  19.03.2019 09:43:27  krbtgt/LOCAL.LNXORG@LOCAL.LNXORG
        renew until 19.03.2019 23:43:27
```

Maintenant nous pouvons nous connecter au serveur en utilisant l'authentification Kerberos SSH.

```
$ ssh kdc.local.com
```