

TP1 : Mise en place de Kerberos et Test**Objectifs :**

- Mettre en place le serveur Kerberos
- Mettre en place le Client
- Faire les tests

1. Mettre à jours les dépendances

```
root@kamailioims:~# apt update
Réception de :1 http://security.ubuntu.com/ubuntu focal-security InRelease [114
kB]
Atteint :2 http://sn.archive.ubuntu.com/ubuntu focal InRelease
Réception de :3 http://sn.archive.ubuntu.com/ubuntu focal-updates InRelease [114
kB]
```

2. Configurer la résolution du nom d'hôte

Tout d'abord, on doit configurer un nom d'hôte complet sur le serveur et sur la machine cliente. Sur le serveur, définissons le nom d'hôte complet avec la commande suivante :

```
#hostnamectl set-hostname server.lita.sn
```

```
root@kamailioims:~# hostnamectl set-hostname server.lita.sn
root@kamailioims:~#
```

Sur la machine cliente, définissez le nom d'hôte complet avec la commande suivante :

```
#hostnamectl set-hostname client1.lita.sn
```

```
root@asterisk:~# hostnamectl set-hostname client1.lita.sn
root@asterisk:~#
```

Ensuite, on modifie les fichiers /etc/hosts sur les machines (serveur et client1) pour que les entités puissent communiquer à travers des noms de domaines

On ajoute les lignes suivantes sur les deux machines :

```
GNU nano 4.8 /etc/hosts
127.0.0.1    localhost
127.0.1.1    kamailioims

192.168.1.33 server.lita.sn
192.168.1.110 client1.lita.sn
```

```
GNU nano 4.8 /etc/hosts
127.0.0.1    localhost www.ecommerce.sn lita.sn
127.0.1.1    asterisk

192.168.1.33 server.lita.sn
192.168.1.110 client1.lita.sn
```

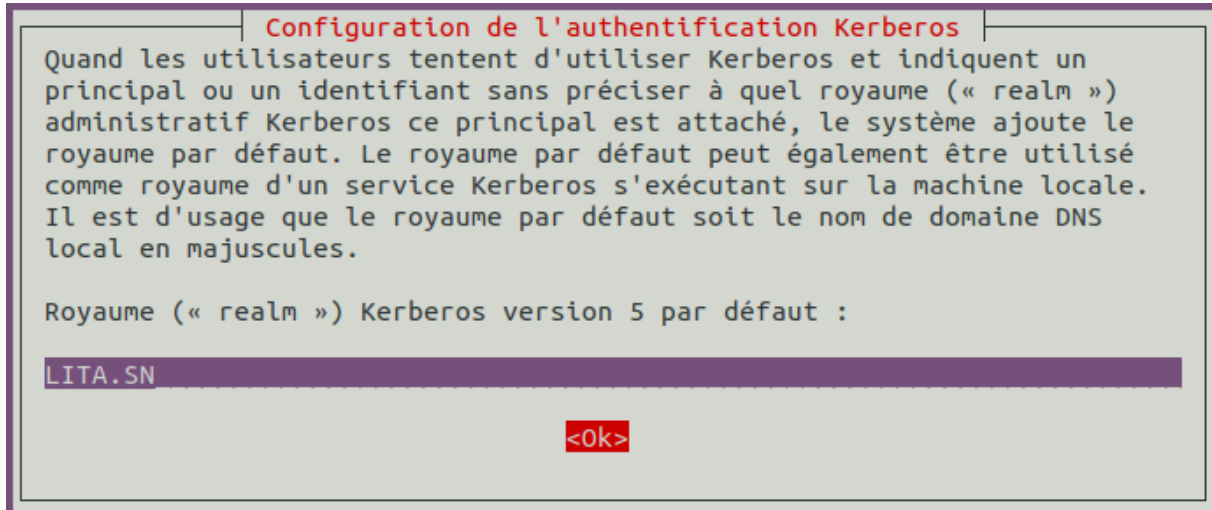
3. Installer le serveur Kerberos

Ensuite, on installe les paquets du serveur Kerberos sur la machine serveur.

```
#apt-get install krb5-kdc krb5-admin-server krb5-config -y
```

```
root@kamailioims:~# apt install krb5-kdc krb5-admin-server krb5-config -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
```

Lors de l'installation, il nous sera demandé de fournir Kerberos Realm, comme indiqué ci-dessous : On renseigne LITA.SN et on clique sur le bouton OK.



Configuration de l'authentification Kerberos

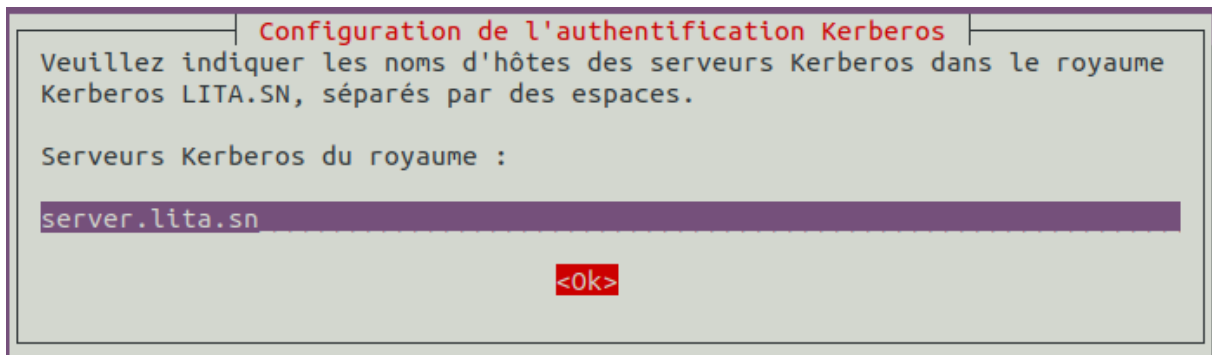
Quand les utilisateurs tentent d'utiliser Kerberos et indiquent un principal ou un identifiant sans préciser à quel royaume (« realm ») administratif Kerberos ce principal est attaché, le système ajoute le royaume par défaut. Le royaume par défaut peut également être utilisé comme royaume d'un service Kerberos s'exécutant sur la machine locale. Il est d'usage que le royaume par défaut soit le nom de domaine DNS local en majuscules.

Royaume (« realm ») Kerberos version 5 par défaut :

LITA.SN

<Ok>

On fournit le nom de domaine complet server.lita.sn + OK .



Configuration de l'authentification Kerberos

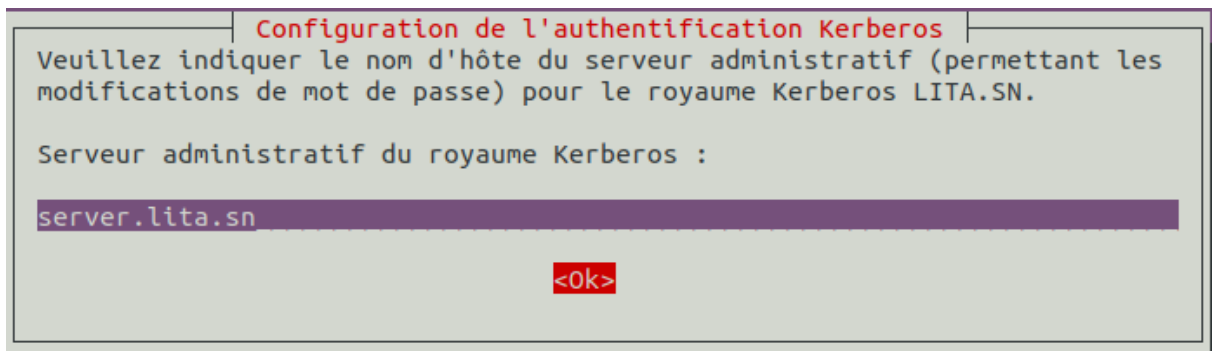
Veuillez indiquer les noms d'hôtes des serveurs Kerberos dans le royaume Kerberos LITA.SN, séparés par des espaces.

Serveurs Kerberos du royaume :

server.lita.sn

<Ok>

Ici aussi on fournit le nom de domaine complet server.lita.sn + OK .



Configuration de l'authentification Kerberos

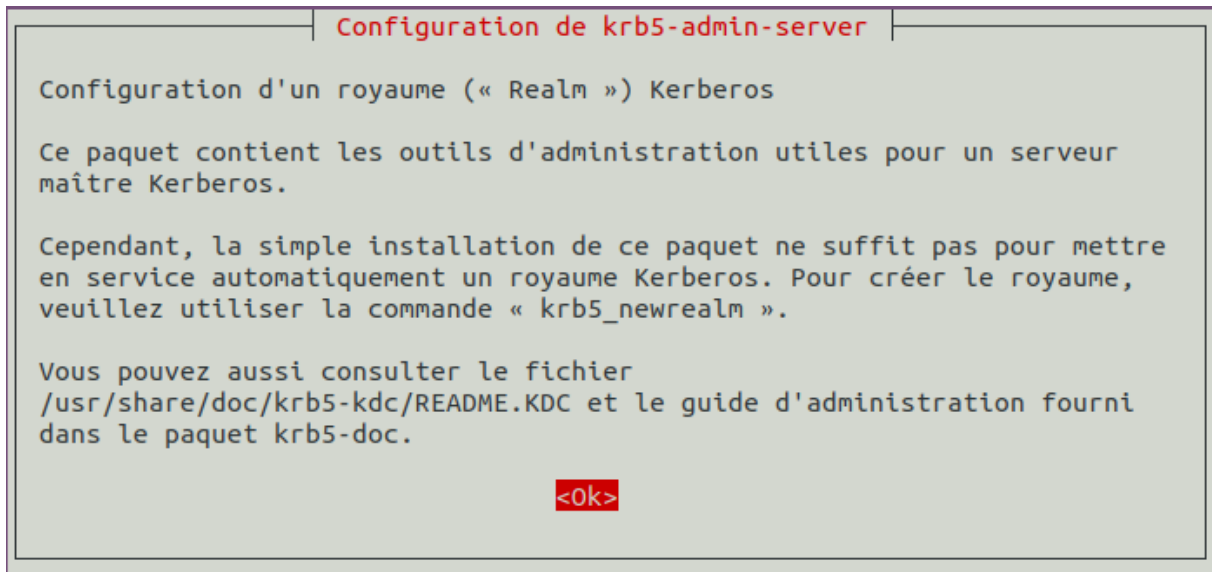
Veuillez indiquer le nom d'hôte du serveur administratif (permettant les modifications de mot de passe) pour le royaume Kerberos LITA.SN.

Serveur administratif du royaume Kerberos :

server.lita.sn

<Ok>

On valide OK pour terminer l'installation



4. Configurer le serveur Kerberos

Après l'installation le serveur ne démarre parce qu'il nous faut d'abord créer un royaume (realm) :

```
See "systemctl status krb5-kdc.service" and "journalctl -xe" for details.
invoke-rc.d: initscript krb5-kdc, action "start" failed.
● krb5-kdc.service - Kerberos 5 Key Distribution Center
   Loaded: loaded (/lib/systemd/system/krb5-kdc.service; enabled; vendor prese
t: enabled)
   Active: failed (Result: exit-code) since Fri 2023-02-24 15:34:09 GMT; 139ms
   ago
   Process: 3643 ExecStart=/usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid $DAEMON_A
RGS (code=exited, status=1/FAILURE)

fee 24 15:34:09 server.lita.sn systemd[1]: Starting Kerberos 5 Key Distribution
Center...
fee 24 15:34:09 server.lita.sn krb5kdc[3643]: Cannot open DB2 database '/var/lib
/krb5kdc/principal': Aucun fichier ou dossier de ce type - while initializing da
```

Pour créer un realm on utilise la commande suivante : **krb5_newrealm**

Il nous sera demandé de fournir un mot de passe comme indiqué ci-dessous :

```
root@kamailioims:~# krb5_newrealm
This script should be run on the master KDC/admin server to initialize
a Kerberos realm. It will ask you to type in a master key password.
This password will be used to generate a key that is stored in
/etc/krb5kdc/stash. You should try to remember this password, but it
is much more important that it be a strong password than that it be
remembered. However, if you lose the password and /etc/krb5kdc/stash,
you cannot decrypt your Kerberos database.
Loading random data
Initializing database '/var/lib/krb5kdc/principal' for realm 'LITA.SN',
master key name 'K/M@LITA.SN'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

```

root@kamailioims:~# krb5_newrealm
This script should be run on the master KDC/admin server to initialize
a Kerberos realm. It will ask you to type in a master key password.
This password will be used to generate a key that is stored in
/etc/krb5kdc/stash. You should try to remember this password, but it
is much more important that it be a strong password than that it be
remembered. However, if you lose the password and /etc/krb5kdc/stash,
you cannot decrypt your Kerberos database.
Loading random data
Initializing database '/var/lib/krb5kdc/principal' for realm 'LITA.SN',
master key name 'K/M@LITA.SN'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:

Now that your realm is set up you may wish to create an administrative
principal using the addprinc subcommand of the kadmin.local program.
Then, this principal can be added to /etc/krb5kdc/kadm5.acl so that
you can use the kadmin program on other computers. Kerberos admin
principals usually belong to a single user and end in /admin. For
example, if juser is a Kerberos administrator, then in addition to
the normal juser principal, a juser/admin principal should be
created.

Don't forget to set up DNS information so your clients can find your
KDC and admin servers. Doing so is documented in the administration
guide.

```

Ensuite, vous devrez ajouter le principal admin à la base de données Kerberos. Vous pouvez le faire avec la commande suivante : **kadmin.local**

Vous devriez voir la sortie suivante :

#addprinc root/admin « ajout d'un principal user admin »

#addprinc -randkey host/server.lita.sn « ajout d'un principal service »

#ktadd host/server.lita.sn « extraire la clé du KDC et la stocker dans le serveur »

```

root@kamailioims:~# kadmin.local
Authenticating as principal root/admin@LITA.SN with password.
kadmin.local: passer
kadmin.local: Unknown request "passer". Type "?" for a request list.
kadmin.local: addprinc -randkey host/server.lita.sn
WARNING: no policy specified for host/server.lita.sn@LITA.SN; defaulting to no
policy
Principal "host/server.lita.sn@LITA.SN" created.
kadmin.local: ktadd host/server.lita.sn
Entry for principal host/server.lita.sn with kvno 2, encryption type aes256-cts
-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/server.lita.sn with kvno 2, encryption type aes128-cts
-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
kadmin.local: quit

```

On ajoute le principe de l'utilisateur administrateur au contrôle d'accès.

nano /etc/krb5kdc/kadm5.acl Ajout de la ligne suivante à la fin :

root/admin *

```

GNU nano 4.8 /etc/krb5kdc/kadm5.acl Modifié
# This file is the access control list for krb5 administration.
# When this file is edited run service krb5-admin-server restart to activate
# One common way to set up Kerberos administration is to allow any principal
# ending in /admin is given full administrative rights.
# To enable this, uncomment the following line:
# */admin *
root/admin *

```

On redémarre le serveur par la commande : `systemctl restart krb5-admin-server`

```

root@kamailioims:~# systemctl restart krb5-admin-server
root@kamailioims:~#

```

On vérifie le statut de krb : `systemctl status krb5-admin-server`

```

root@kamailioims:~# systemctl status krb5-admin-server
● krb5-admin-server.service - Kerberos 5 Admin Server
   Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; v>
   Active: active (running) since Fri 2023-02-24 15:55:13 GMT; 58s ago
     Main PID: 4718 (kadmind)
        Tasks: 1 (limit: 4618)
       Memory: 644.0K
          CGroup: /system.slice/krb5-admin-server.service
                 └─4718 /usr/sbin/kadmind -nofork

fee 24 15:55:13 server.lita.sn kadmind[4718]: Setting up TCP socket for address>
fee 24 15:55:13 server.lita.sn kadmind[4718]: Setting up TCP socket for address>
fee 24 15:55:13 server.lita.sn kadmind[4718]: setsockopt(12,IPV6_V6ONLY,1) wor>
fee 24 15:55:13 server.lita.sn kadmind[4718]: Setting up RPC socket for address>
fee 24 15:55:13 server.lita.sn kadmind[4718]: Setting up RPC socket for address>
fee 24 15:55:13 server.lita.sn kadmind[4718]: setsockopt(14,IPV6_V6ONLY,1) wor>
fee 24 15:55:13 server.lita.sn kadmind[4718]: set up 6 sockets
fee 24 15:55:13 server.lita.sn kadmind[4718]: Seeding random number generator
fee 24 15:55:13 server.lita.sn kadmind[4718]: starting
fee 24 15:55:13 server.lita.sn kadmind[4718]: kadmind: starting...
lines 1-19/19 (END)

```

5. Configuration du client Kerberos

Configuration de FQDN du client

```
#hostnamectl set-hostname client1.lita.sn
```

Installation du client kerberos

Les paquets à installer :

```
#apt install krb5-user libpam-krb5 libpam-ccreds auth-client-config
```



```
root@asterisk:~# apt install krb5-user libpam-krb5 libpam-ccreds
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  libxmb1
Veuillez utiliser « apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
  krb5-config
Paquets suggérés :
  krb5-k5tls nss-updatedb
Les NOUVEAUX paquets suivants seront installés :
  krb5-config krb5-user libpam-ccreds libpam-krb5
0 mis à jour, 4 nouvellement installés, 0 à enlever et 44 non mis à jour.
Il est nécessaire de prendre 225 ko dans les archives.
Après cette opération, 796 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

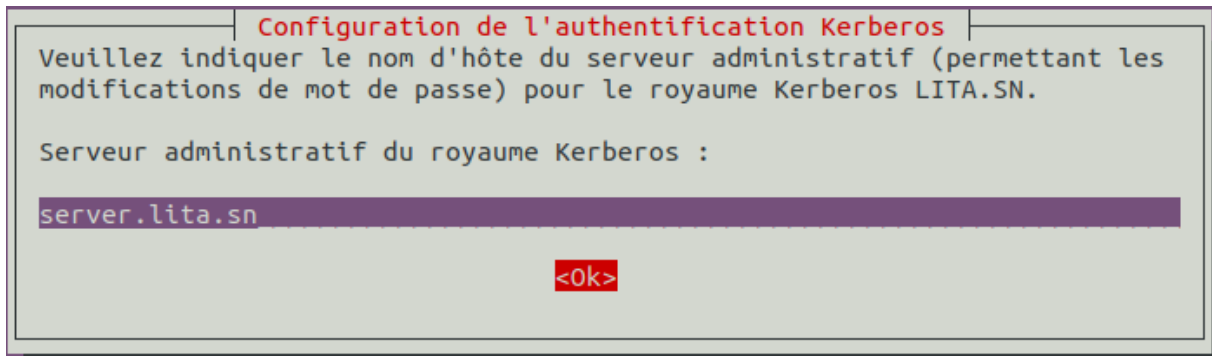
On renseigne le realm (LITA.SN) et le nom de domaine du serveur.

Configuration de l'authentification Kerberos	
Quand les utilisateurs tentent d'utiliser Kerberos et indiquent un principal ou un identifiant sans préciser à quel royaume (« realm ») administratif Kerberos ce principal est attaché, le système ajoute le royaume par défaut. Le royaume par défaut peut également être utilisé comme royaume d'un service Kerberos s'exécutant sur la machine locale. Il est d'usage que le royaume par défaut soit le nom de domaine DNS local en majuscules.	
Royaume (« realm ») Kerberos version 5 par défaut :	
<input type="text" value="LITA.SN"/>	
<input type="button" value="Ok"/>	

On fournit le nom de domaine du serveur

Configuration de l'authentification Kerberos	
Veuillez indiquer les noms d'hôtes des serveurs Kerberos dans le royaume Kerberos LITA.SN, séparés par des espaces.	
Serveurs Kerberos du royaume :	
<input type="text" value="server.lita.sn"/>	
<input type="button" value="Ok"/>	

On renseigne encore le nom de domaine défini sur la machine serveur



À partir de la machine cliente on test la connectivité par la commande : kadmin pour ajouter le principal service de la machine cliente

```
#addprinc -randkey host/client1.lita.sn
```

6. Test client/serveur Kerberos

Configurer le serveur 'server.rtn.sn' en ajoutant un compte

L'ajout du compte ndoumbe sur le serveur par la commande :

```
#useradd -m -s /bin/bash ndoumbe
```

```
root@kamailioims:~# useradd -m -s /bin/bash ndoumbe
root@kamailioims:~#
```

On teste par la commande : kadmin.local

```
#addprinc ndoumbe
```

```
root@kamailioims:~# kadmin.local
Authenticating as principal root/admin@LITA.SN with password.
kadmin.local: passer
kadmin.local: Unknown request "passer". Type "?" for a request list.
kadmin.local: addprinc ndoumbe
WARNING: no policy specified for ndoumbe@LITA.SN; defaulting to no policy
Enter password for principal "ndoumbe@LITA.SN":
Re-enter password for principal "ndoumbe@LITA.SN":
Principal "ndoumbe@LITA.SN" created.
kadmin.local: quit
```

On édite le fichier /etc/ssh/sshd_config pour décommenter les deux lignes suivantes :

```
#GSSAPIAuthentication yes
```

```
#GSSAPICleanupCredentials yes
```

```

GNU nano 4.8 /etc/ssh/ssh_config
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes

```

Puis on redémarre sshd : `systemctl restart sshd`

Configurer la machine 'client1.lita.sn'

Ajout de l'utilisateur ndoumbe sur la machine cliente

`#useradd -m -s /bin/bash ndoumbe`

On vient d'ajouter le compte ndoumbe sur la machine cliente et ensuite on se connecte au compte ndoumbe par la commande `su - ndoumbe`

```

root@asterisk:~# su - ndoumbe
ndoumbe@client1:~$

```

On fait kinit ndoumbe

```

root@server:~# su - ndoumbe
ndoumbe@server:~$ kinit ndoumbe
Password for ndoumbe@LITA.SN:
ndoumbe@server:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: ndoumbe@LITA.SN

Valid starting    Expires          Service principal
28.02.2023 15:28:07  01.03.2023 01:28:07  krbtgt/LITA.SN@LITA.SN
        renew until 01.03.2023 15:28:04
ndoumbe@server:~$

```