TÉLÉCOMMUNICATION ET RÉSEAUX

LICENCE 3

ANNÉE-SCOLAIRE 2023 – 2024

Rapport Système d'Authentification Centralisé avec FreeRadius, LDAP et Kerberos

Etudiant **:** Enseignant :

Yacine Mbaye Dr Keba GUEYE

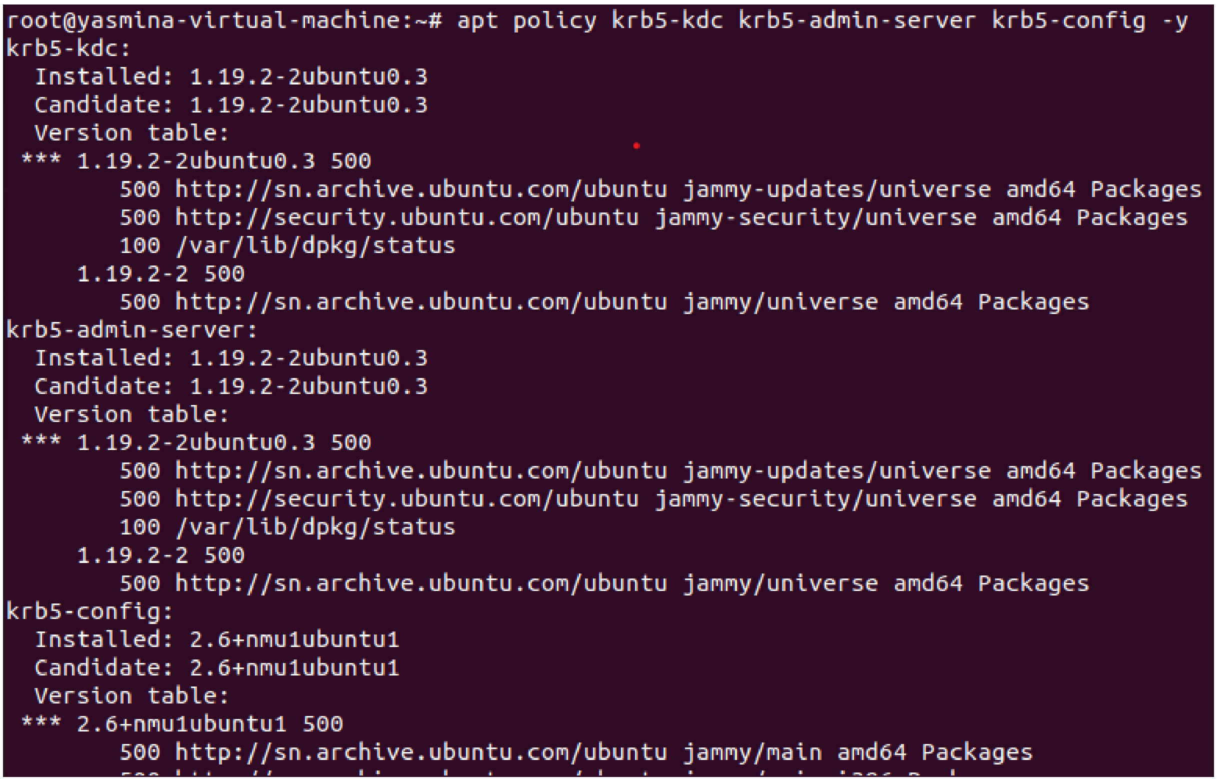
Objectif :

Ce projet vise à concevoir, implémenter et sécuriser un système d'authentification centralisé. Ce système utilisera FreeRadius pour la gestion des requêtes d'authentification, LDAP pour le stockage des informations des utilisateurs, et Kerberos pour assurer une authentification sécurisée. L'objectif est de fournir une authentification forte et centralisée pour divers services réseau.

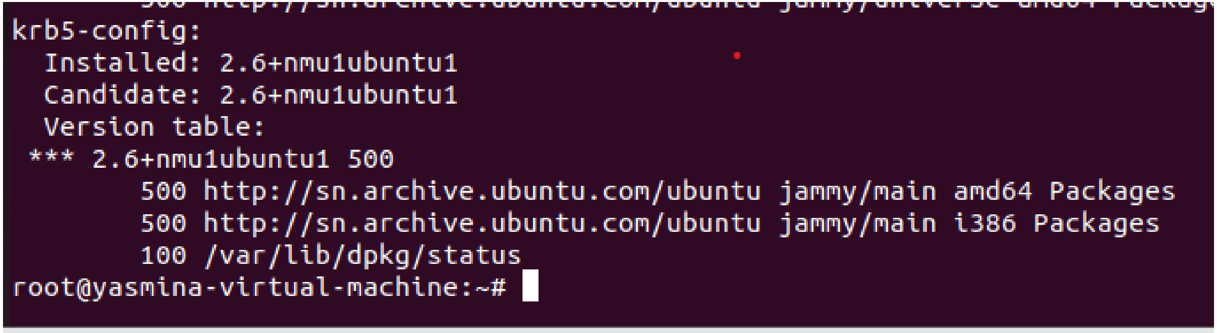
Mise en œuvre :

1. Installation des paquets

Pour KERBEROS

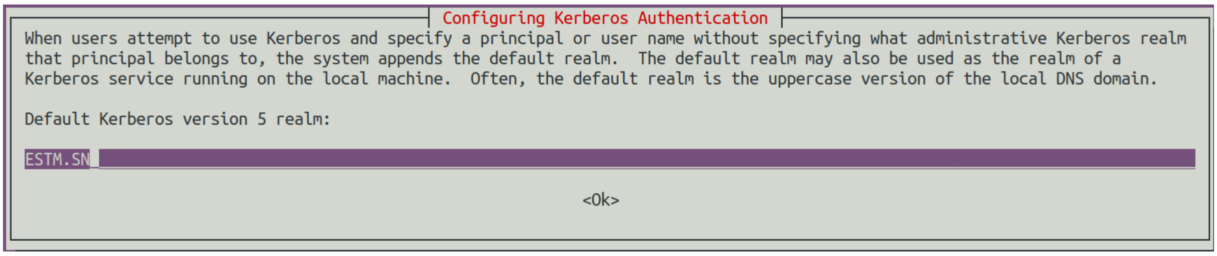


```
root@yasmina-virtual-machine:~# apt policy krb5-kdc krb5-admin-server krb5-config -y
krb5-kdc:
  Installed: 1.19.2-2ubuntu0.3
  Candidate: 1.19.2-2ubuntu0.3
  Version table:
 *** 1.19.2-2ubuntu0.3 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages
        500 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages
        100 /var/lib/dpkg/status
     1.19.2-2 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages
krb5-admin-server:
  Installed: 1.19.2-2ubuntu0.3
  Candidate: 1.19.2-2ubuntu0.3
  Version table:
 *** 1.19.2-2ubuntu0.3 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages
        500 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages
        100 /var/lib/dpkg/status
     1.19.2-2 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages
krb5-config:
  Installed: 2.6+nmu1ubuntu1
  Candidate: 2.6+nmu1ubuntu1
  Version table:
 *** 2.6+nmu1ubuntu1 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 Packages
```



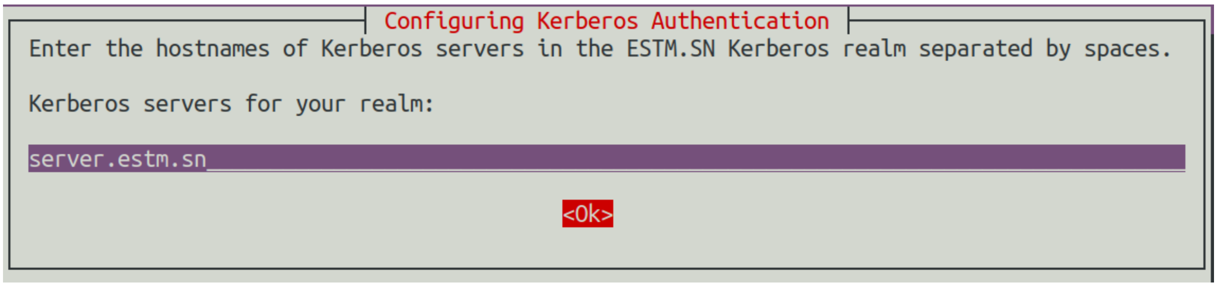
```
krb5-config:
  Installed: 2.6+nmu1ubuntu1
  Candidate: 2.6+nmu1ubuntu1
  Version table:
 *** 2.6+nmu1ubuntu1 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 Packages
        500 http://sn.archive.ubuntu.com/ubuntu jammy/main i386 Packages
        100 /var/lib/dpkg/status
root@yasmina-virtual-machine:~# 
```

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



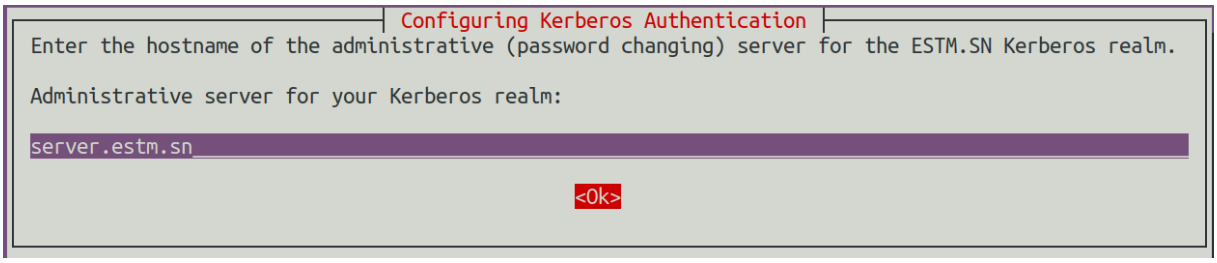
```
Configuring Kerberos Authentication
When users attempt to use Kerberos and specify a principal or user name without specifying what administrative Kerberos realm
that principal belongs to, the system appends the default realm.  The default realm may also be used as the realm of a
Kerberos service running on the local machine.  Often, the default realm is the uppercase version of the local DNS domain.

Default Kerberos version 5 realm:

ESTM.SN_

<Ok>
```

- On fournit le nom de domaine complet server.estm.sn



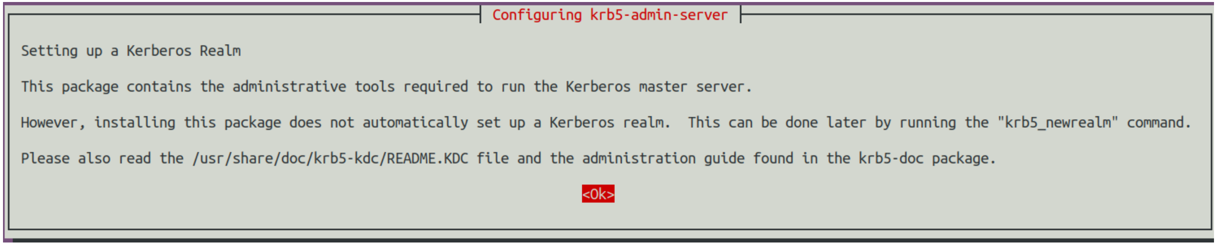
```
Configuring Kerberos Authentication
Enter the hostnames of Kerberos servers in the ESTM.SN Kerberos realm separated by spaces.

Kerberos servers for your realm:

server.estm.sn_

<Ok>
```

- Aussi on fournit le nom de domaine complet server.estm.sn



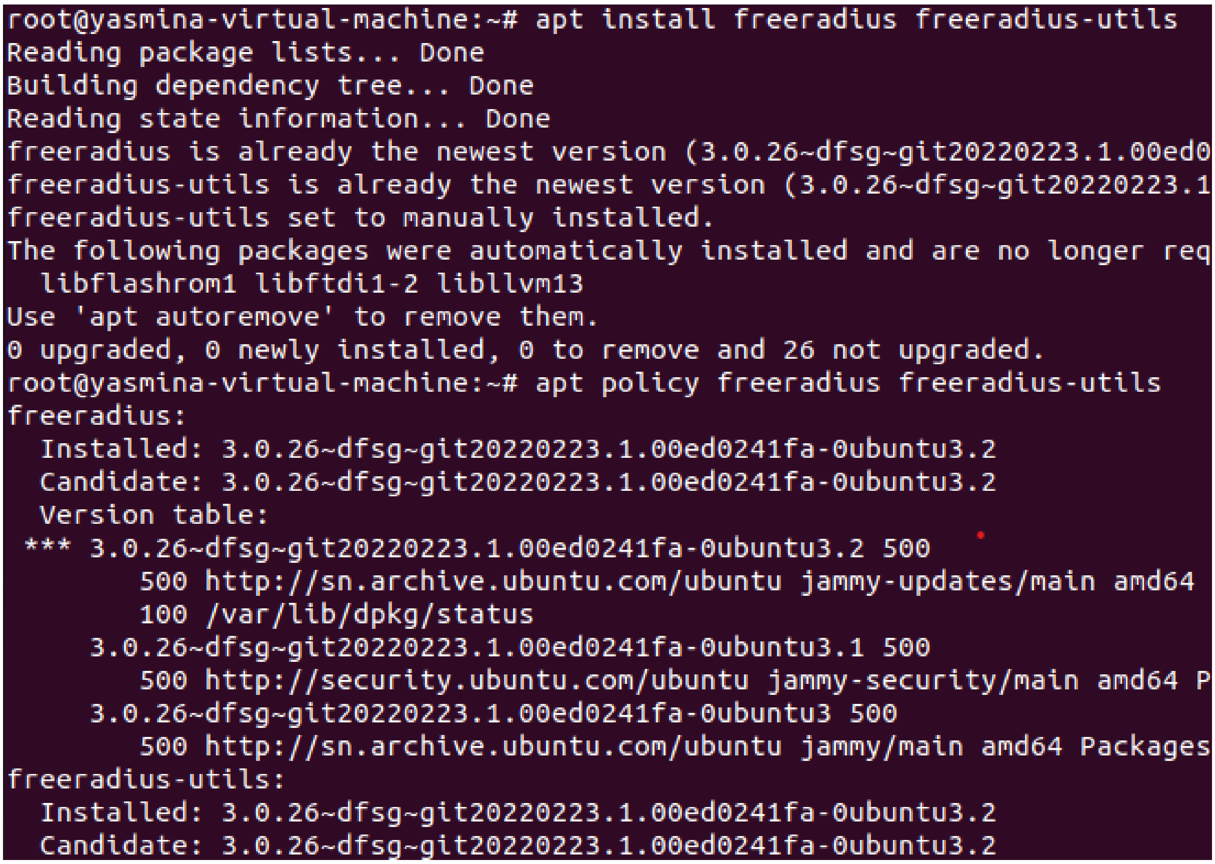
```
Configuring Kerberos Authentication
Enter the hostname of the administrative (password changing) server for the ESTM.SN Kerberos realm.

Administrative server for your Kerberos realm:

server.estm.sn_

<Ok>
```

- On valide OK pour terminer l'installation

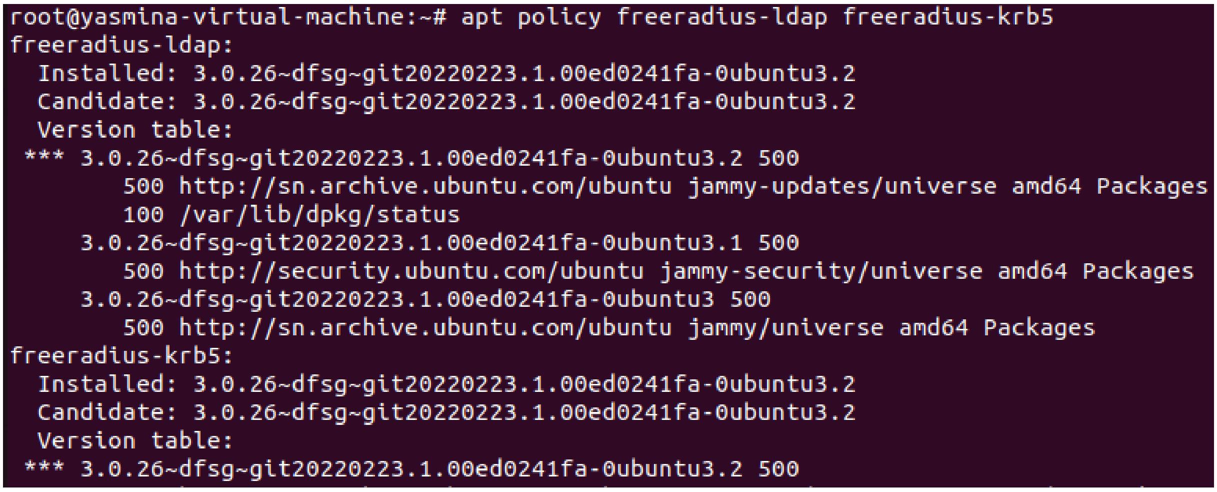


```
Configuring krb5-admin-server

Setting up a Kerberos Realm

This package contains the administrative tools required to run the Kerberos master server.

However, installing this package does not automatically set up a Kerberos realm.  This can be done later by running the "krb5_newrealm" command.

Please also read the /usr/share/doc/krb5-kdc/README.KDC file and the administration guide found in the krb5-doc package.

<Ok>
```

Pour FREERADIUS

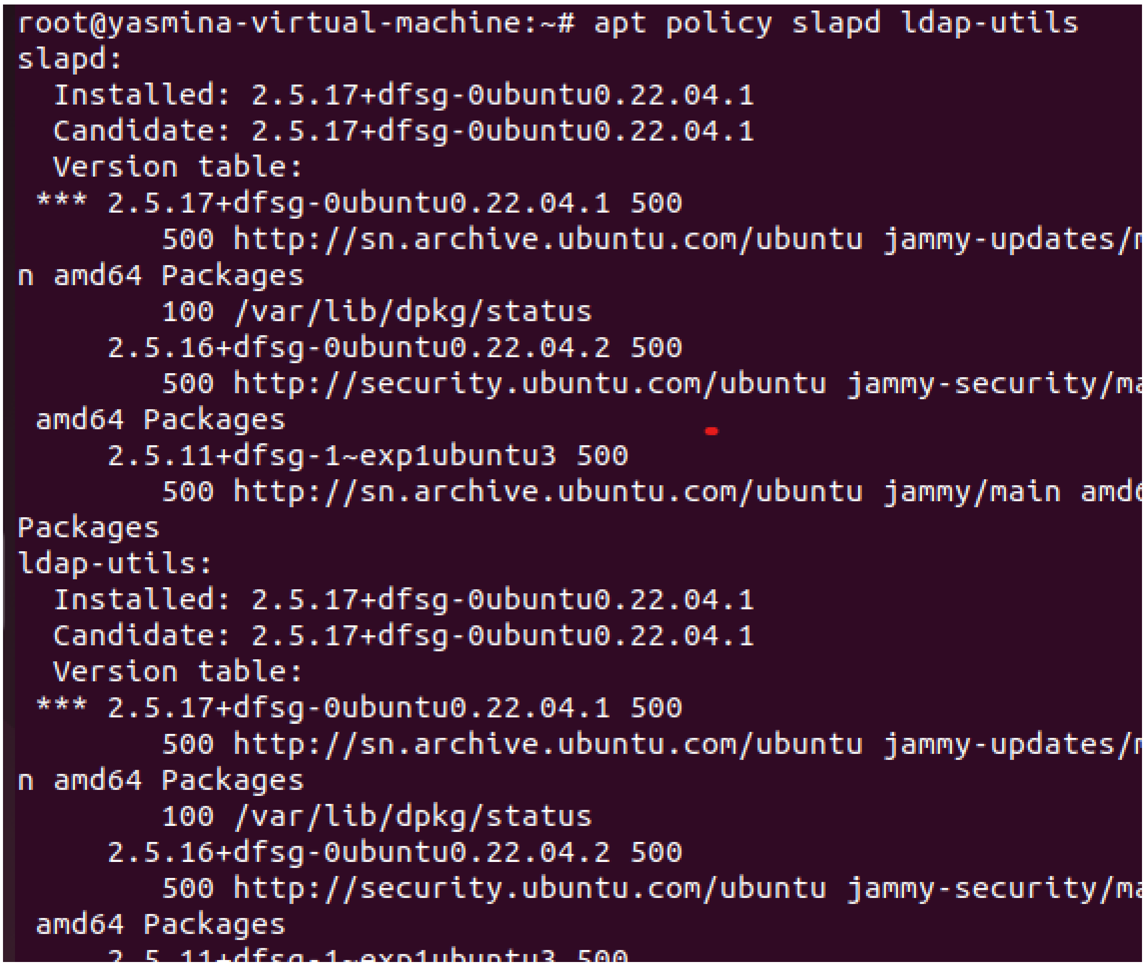


```
root@yasmina-virtual-machine:~# apt install freeradius freeradius-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
freeradius is already the newest version (3.0.26~dfsg~git20220223.1.00ed0
freeradius-utils is already the newest version (3.0.26~dfsg~git20220223.1
freeradius-utils set to manually installed.
The following packages were automatically installed and are no longer req
  libflashrom1 libftdi1-2 libllvm13
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.
root@yasmina-virtual-machine:~# apt policy freeradius freeradius-utils
freeradius:
  Installed: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Candidate: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Version table:
 *** 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/main amd64
        100 /var/lib/dpkg/status
     3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.1 500
        500 http://security.ubuntu.com/ubuntu jammy-security/main amd64 P
     3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 Packages
freeradius-utils:
  Installed: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Candidate: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
```

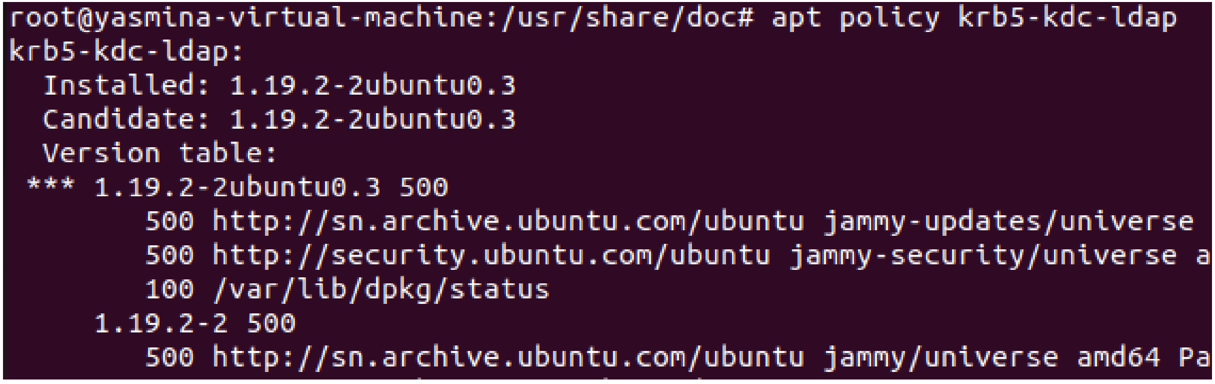


```
root@yasmina-virtual-machine:~# apt policy freeradius-ldap freeradius-krb5
freeradius-ldap:
  Installed: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Candidate: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Version table:
 *** 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages
        100 /var/lib/dpkg/status
     3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.1 500
        500 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages
     3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages
freeradius-krb5:
  Installed: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Candidate: 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2
  Version table:
 *** 3.0.26~dfsg~git20220223.1.00ed0241fa-0ubuntu3.2 500
```

Pour LDAP



```
root@yasmina-virtual-machine:~# apt policy slapd ldap-utils
slapd:
  Installed: 2.5.17+dfsg-0ubuntu0.22.04.1
  Candidate: 2.5.17+dfsg-0ubuntu0.22.04.1
  Version table:
 *** 2.5.17+dfsg-0ubuntu0.22.04.1 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/m
n amd64 Packages
        100 /var/lib/dpkg/status
     2.5.16+dfsg-0ubuntu0.22.04.2 500
        500 http://security.ubuntu.com/ubuntu jammy-security/ma
 amd64 Packages
     2.5.11+dfsg-1~exp1ubuntu3 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/main amd6
Packages
ldap-utils:
  Installed: 2.5.17+dfsg-0ubuntu0.22.04.1
  Candidate: 2.5.17+dfsg-0ubuntu0.22.04.1
  Version table:
 *** 2.5.17+dfsg-0ubuntu0.22.04.1 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/m
n amd64 Packages
        100 /var/lib/dpkg/status
     2.5.16+dfsg-0ubuntu0.22.04.2 500
        500 http://security.ubuntu.com/ubuntu jammy-security/ma
 amd64 Packages
     2.5.11+dfsg-1~exp1ubuntu3 500
```

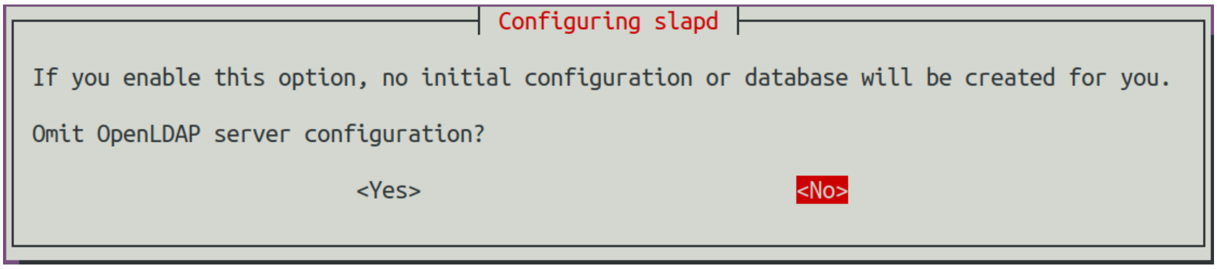


```
root@yasmina-virtual-machine:/usr/share/doc# apt policy krb5-kdc-ldap
krb5-kdc-ldap:
  Installed: 1.19.2-2ubuntu0.3
  Candidate: 1.19.2-2ubuntu0.3
  Version table:
 *** 1.19.2-2ubuntu0.3 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy-updates/universe
        500 http://security.ubuntu.com/ubuntu jammy-security/universe a
        100 /var/lib/dpkg/status
     1.19.2-2 500
        500 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 Pa
```

2. Configuration de LDAP pour Kerberos

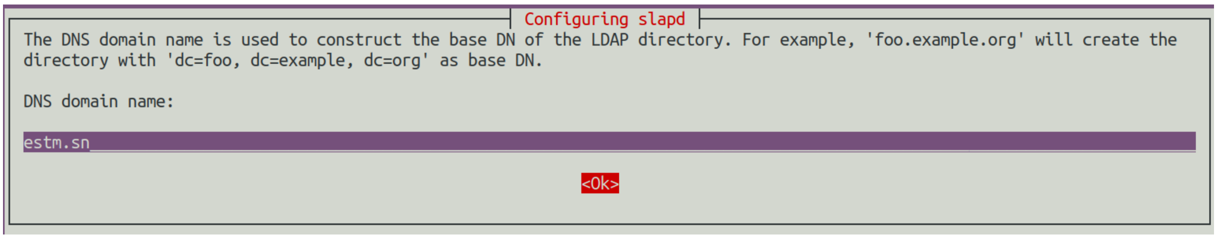
Utilisons la commande **dpkg reconfigure slapd** pour reconfigurer le serveur LDAP.

- Omettre la configuration initiale : Non



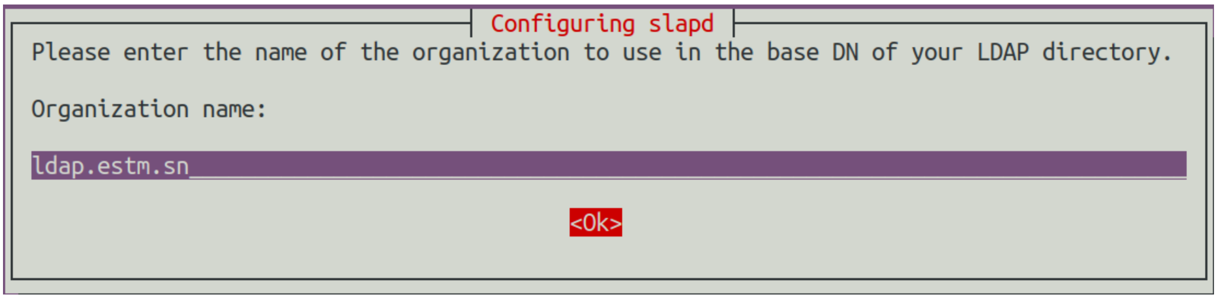
```
Configuring slapd

If you enable this option, no initial configuration or database will be created for you.

Omit OpenLDAP server configuration?

                  <Yes>                          <No>
```

- Nom de domaine DNS : estm.sn



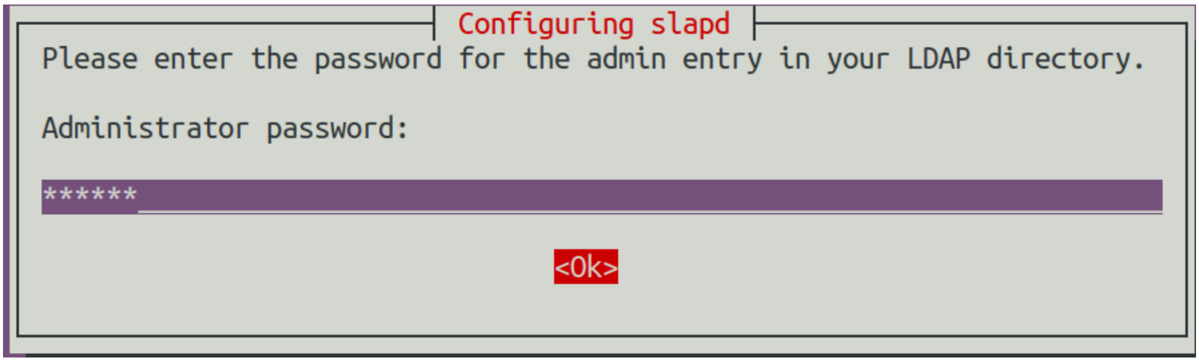
```
Configuring slapd
The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the
directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

estm.sn

<Ok>
```

- Nom de l'organisation : ldap.estm.sn



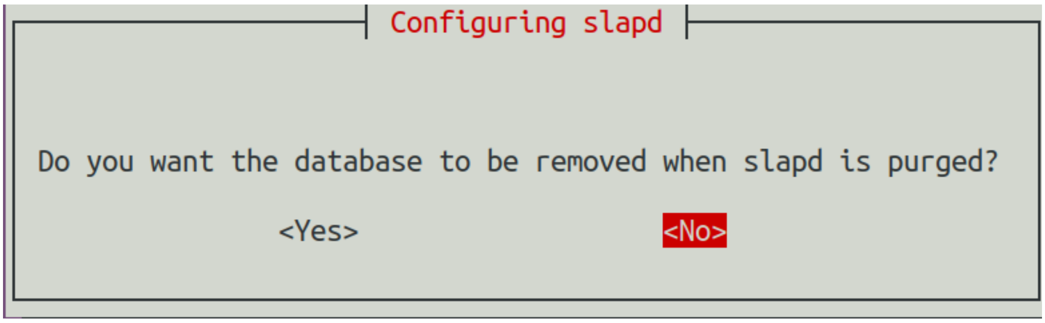
```
Configuring slapd
Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

ldap.estm.sn

<Ok>
```

- Mot de passe administrateur :



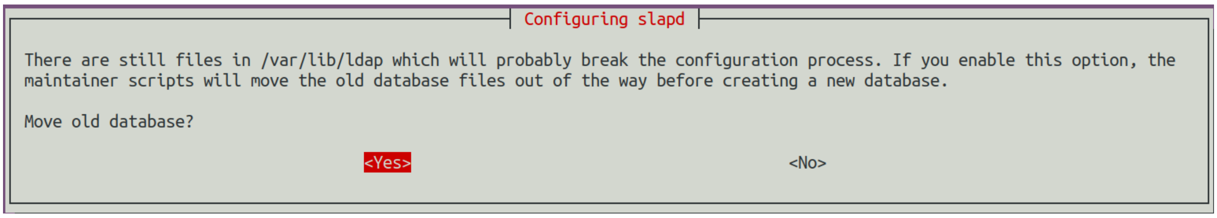
```
Configuring slapd
Please enter the password for the admin entry in your LDAP directory.

Administrator password:

******

<Ok>
```

- Voulez-vous que la base de données soit supprimée lorsque slapd est purgé : Non



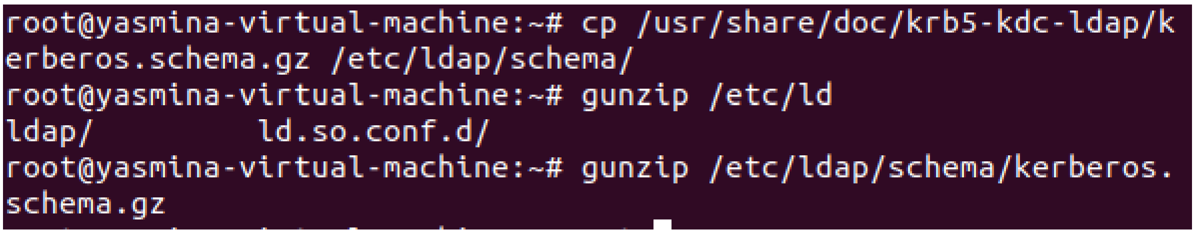
```
Configuring slapd


Do you want the database to be removed when slapd is purged?

          <Yes>                    <No>
```

- Déplacer l'ancienne base de données : Oui



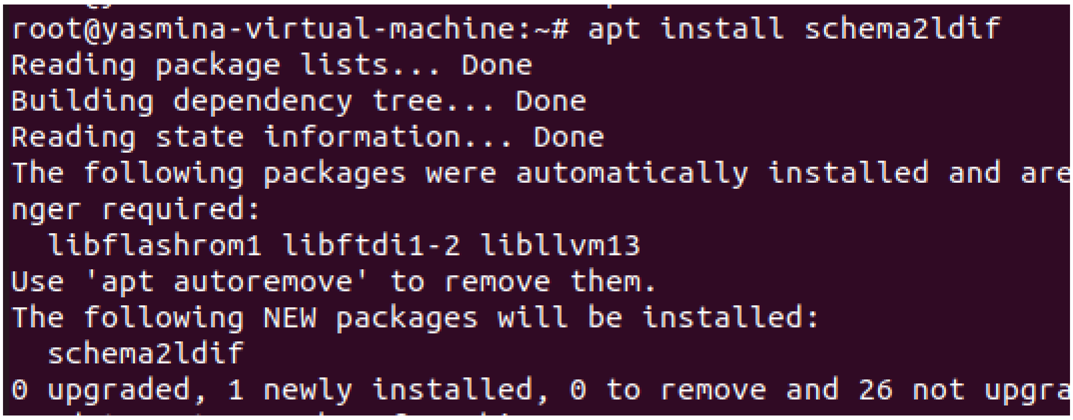
```
Configuring slapd

There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the
maintainer scripts will move the old database files out of the way before creating a new database.

Move old database?

                    <Yes>                                        <No>
```

- Copions le schéma dans /etc/ldap/schema et extrayons le fichier kerberos.schema.gz



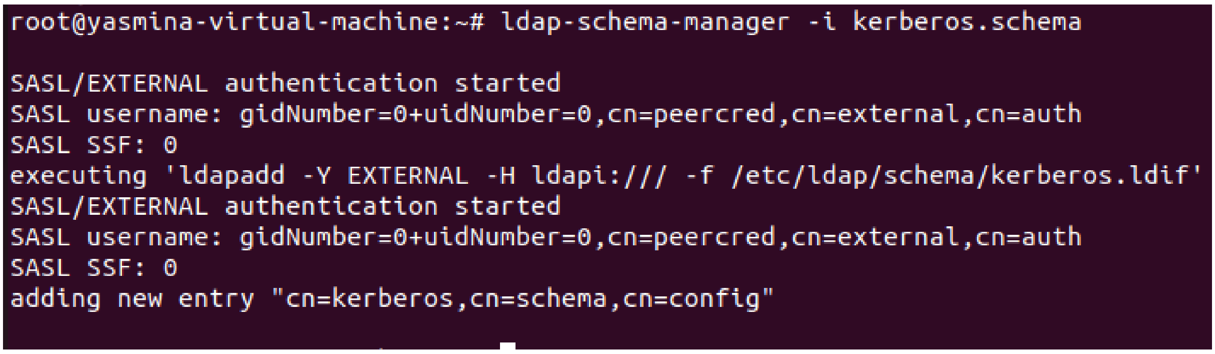
```
root@yasmina-virtual-machine:~# cp /usr/share/doc/krb5-kdc-ldap/k
erberos.schema.gz /etc/ldap/schema/
root@yasmina-virtual-machine:~# gunzip /etc/ld
ldap/          ld.so.conf.d/
root@yasmina-virtual-machine:~# gunzip /etc/ldap/schema/kerberos.
schema.gz
```

- Le schéma Kerberos doit être ajouté au cn=configarborescence. Ce fichier de schéma doit être converti au format LDIF avant de pouvoir être ajouté. Pour cela nous utiliserons un outil d'assistance, appelé schema2ldif, fourni par le package du même nom qui est disponible dans l'archive Universe :



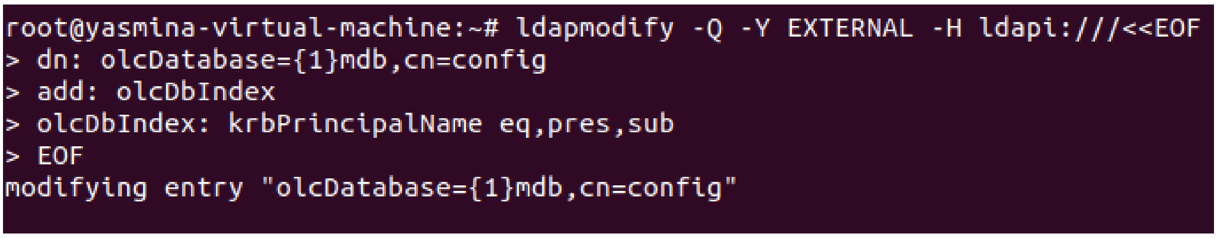
```
root@yasmina-virtual-machine:~# apt install schema2ldif
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are
nger required:
  libflashrom1 libftdi1-2 libllvm13
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  schema2ldif
0 upgraded, 1 newly installed, 0 to remove and 26 not upgra
```

- Importation du schéma Kerberos
- Importation du schéma Kerberos



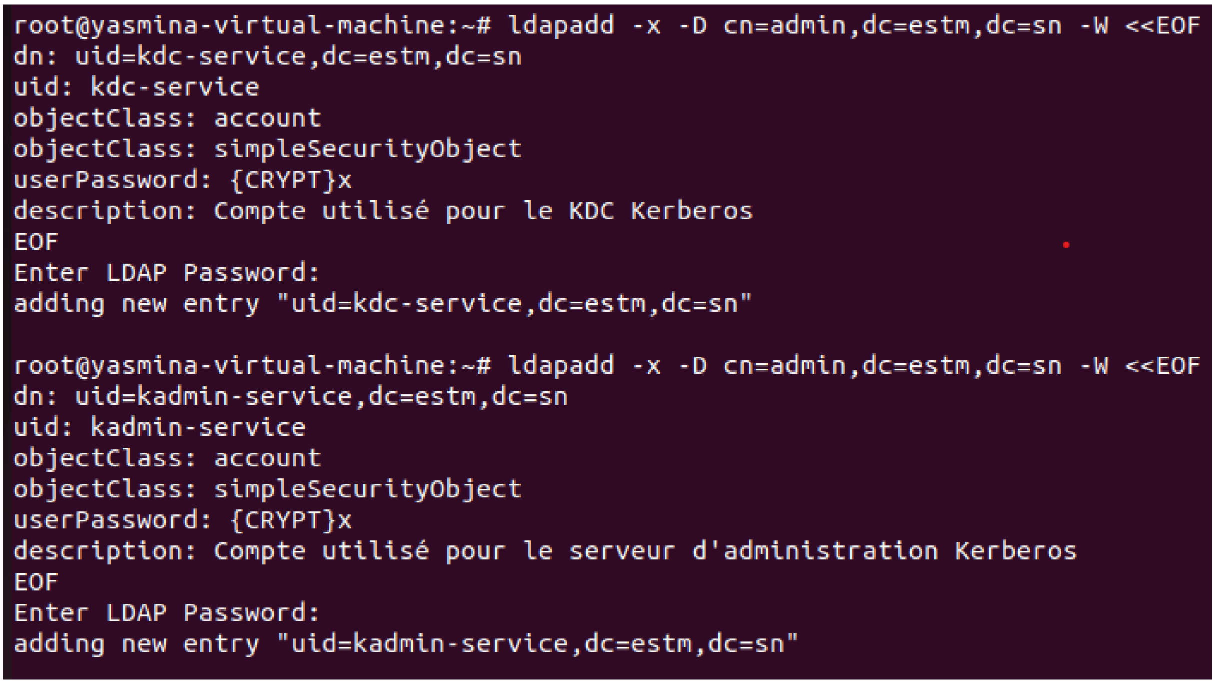
```
root@yasmina-virtual-machine:~# ldap-schema-manager -i kerberos.schema

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/kerberos.ldif'
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=kerberos,cn=schema,cn=config"
```

- Une fois le nouveau schéma chargé, indexons un attribut souvent utilisé dans les recherches



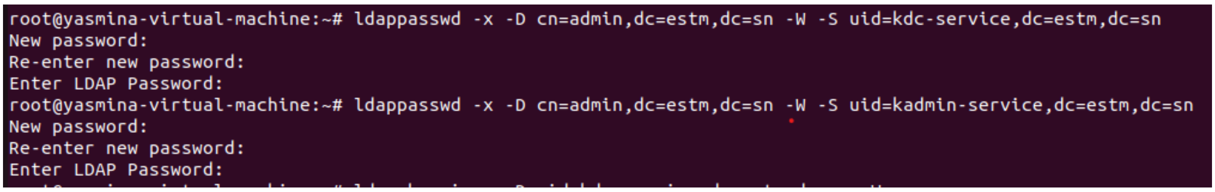
```
root@yasmina-virtual-machine:~# ldapmodify -Q -Y EXTERNAL -H ldapi:///<<EOF
> dn: olcDatabase={1}mdb,cn=config
> add: olcDbIndex
> olcDbIndex: krbPrincipalName eq,pres,sub
> EOF
modifying entry "olcDatabase={1}mdb,cn=config"
```

- Créons des entrées LDAP pour les entités administratives Kerberos qui contacteront le serveur OpenLDAP pour effectuer des opérations. Il y en a deux:
- **ldap_kdc_dn:** qui doit avoir des droits de lecture sur le conteneur de domaine, le conteneur principal et les sous-arborescences de domaine. Cependant, si disable_last_success et disable_lockoutne sont pas définis, ldap_kdc_dn nécessite un accès en écriture au conteneur Kerberos, tout comme le DN d'administrateur ci-dessous.
- **ldap_kadmind_dn** : qui doit avoir des droits de lecture et d'écriture sur le conteneur de domaine, le conteneur principal et les sous-arborescences de domaine



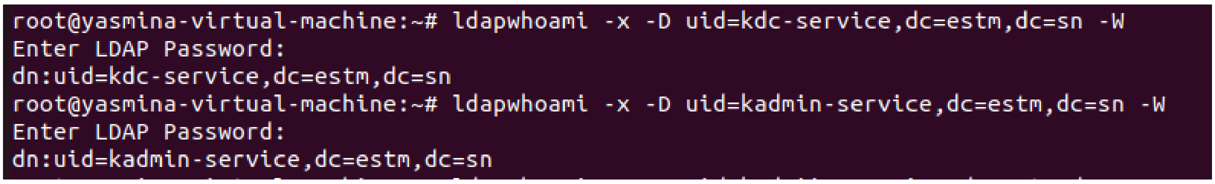
```
root@yasmina-virtual-machine:~# ldapadd -x -D cn=admin,dc=estm,dc=sn -W <<EOF
dn: uid=kdc-service,dc=estm,dc=sn
uid: kdc-service
objectClass: account
objectClass: simpleSecurityObject
userPassword: {CRYPT}x
description: Compte utilisé pour le KDC Kerberos
EOF
Enter LDAP Password:
adding new entry "uid=kdc-service,dc=estm,dc=sn"

root@yasmina-virtual-machine:~# ldapadd -x -D cn=admin,dc=estm,dc=sn -W <<EOF
dn: uid=kadmin-service,dc=estm,dc=sn
uid: kadmin-service
objectClass: account
objectClass: simpleSecurityObject
userPassword: {CRYPT}x
description: Compte utilisé pour le serveur d'administration Kerberos
EOF
Enter LDAP Password:
adding new entry "uid=kadmin-service,dc=estm,dc=sn"
```

- Maintenant, définissons-leur un mot de passe



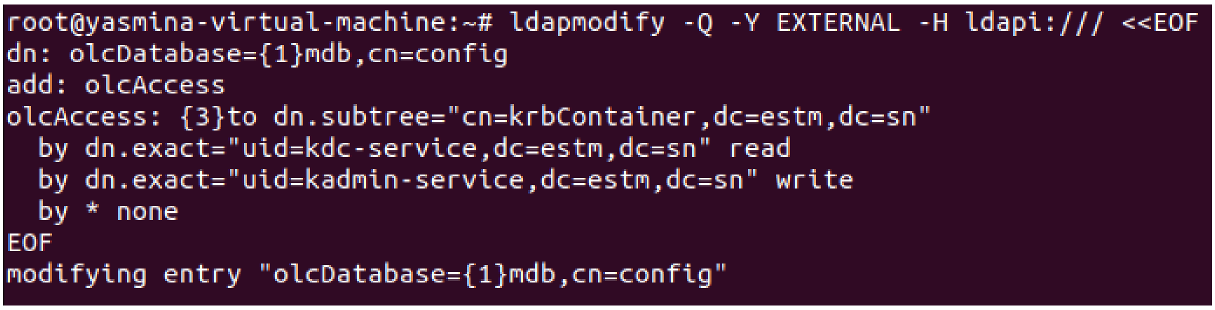
```
root@yasmina-virtual-machine:~# ldappasswd -x -D cn=admin,dc=estm,dc=sn -W -S uid=kdc-service,dc=estm,dc=sn
New password:
Re-enter new password:
Enter LDAP Password:
root@yasmina-virtual-machine:~# ldappasswd -x -D cn=admin,dc=estm,dc=sn -W -S uid=kadmin-service,dc=estm,dc=sn
New password:
Re-enter new password:
Enter LDAP Password:
```

- Faisons le test avec la commande ldapwhoami



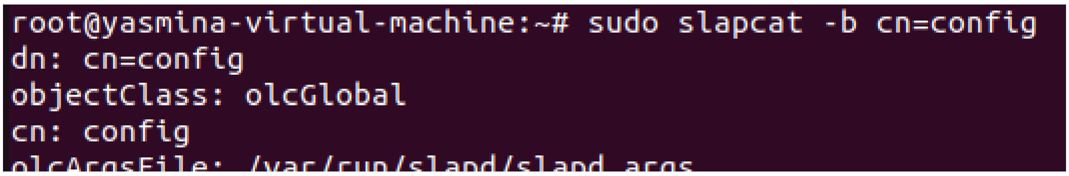
```
root@yasmina-virtual-machine:~# ldapwhoami -x -D uid=kdc-service,dc=estm,dc=sn -W
Enter LDAP Password:
dn:uid=kdc-service,dc=estm,dc=sn
root@yasmina-virtual-machine:~# ldapwhoami -x -D uid=kadmin-service,dc=estm,dc=sn -W
Enter LDAP Password:
dn:uid=kadmin-service,dc=estm,dc=sn
```

- Enfin, mettons à jour les listes de contrôle d’accès (ACL).
  Nous devons insérer les nouvelles règles avant la dernière, pour contrôler l’accès aux entrées et attributs liés à Kerberos

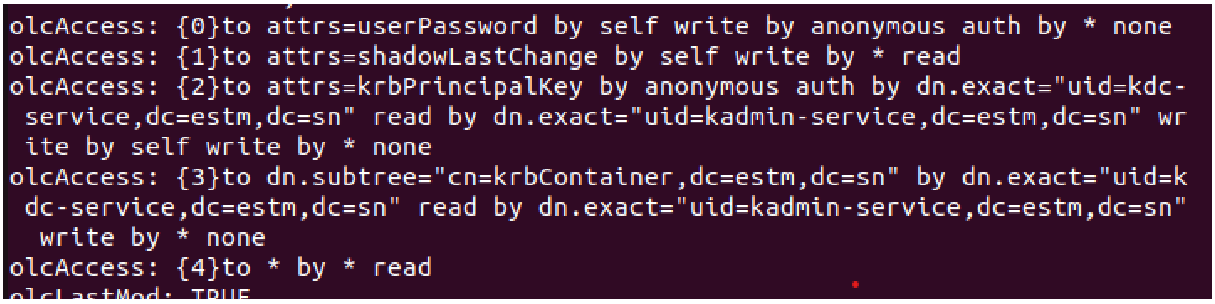


```
root@yasmina-virtual-machine:~# ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF
dn: olcDatabase={1}mdb,cn=config
add: olcAccess
olcAccess: {3}to dn.subtree="cn=krbContainer,dc=estm,dc=sn"
  by dn.exact="uid=kdc-service,dc=estm,dc=sn" read
  by dn.exact="uid=kadmin-service,dc=estm,dc=sn" write
  by * none
EOF
modifying entry "olcDatabase={1}mdb,cn=config"
```

- Vérifions les ACLs avec la commande sudo slapcat -b cn=config



```
root@yasmina-virtual-machine:~# sudo slapcat -b cn=config
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/run/slapd/slapd.args
```

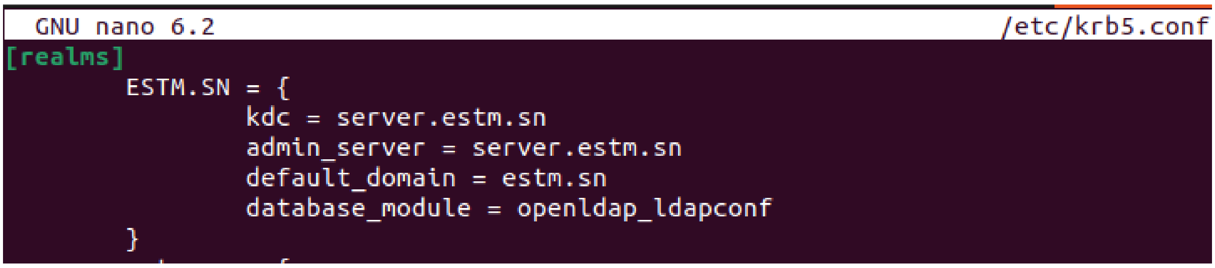


```
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to attrs=krbPrincipalKey by anonymous auth by dn.exact="uid=kdc-
 service,dc=estm,dc=sn" read by dn.exact="uid=kadmin-service,dc=estm,dc=sn" wr
 ite by self write by * none
olcAccess: {3}to dn.subtree="cn=krbContainer,dc=estm,dc=sn" by dn.exact="uid=k
 dc-service,dc=estm,dc=sn" read by dn.exact="uid=kadmin-service,dc=estm,dc=sn"
  write by * none
olcAccess: {4}to * by * read
olcLastMod: TRUE
```

3. Configuration du KDC principal (LDAP)

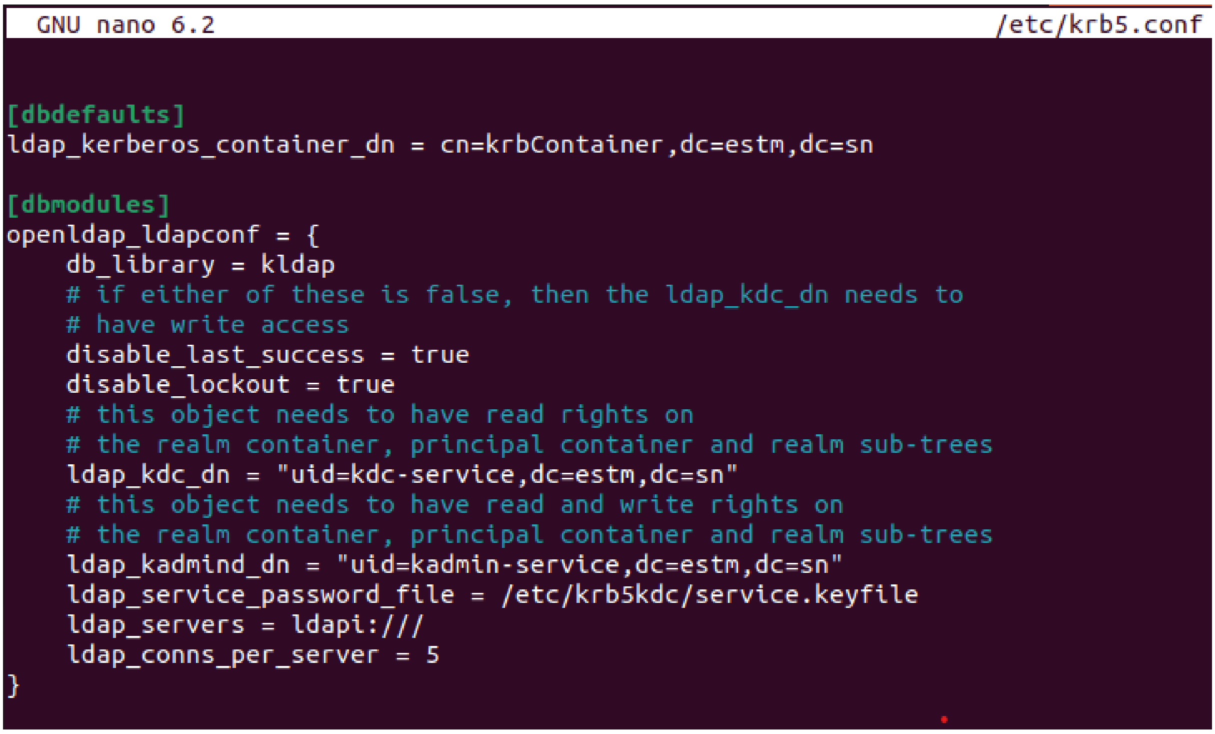
Une fois OpenLDAP configuré, il est temps de configurer le KDC On édite le fichier /etc/krb5.conf en rajoutant les paramètres suivants dans la section [realms]

default_domain = server.estm.sn
database_module = openldap_ldapconf



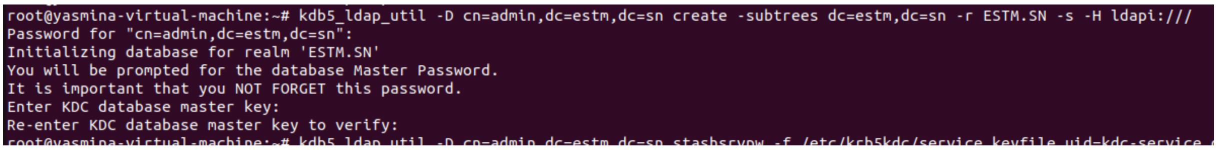
```
[realms]
        ESTM.SN = {
                kdc = server.estm.sn
                admin_server = server.estm.sn
                default_domain = estm.sn
                database_module = openldap_ldapconf
        }
```

- Ensuite, on ajoute également ces nouvelles sections



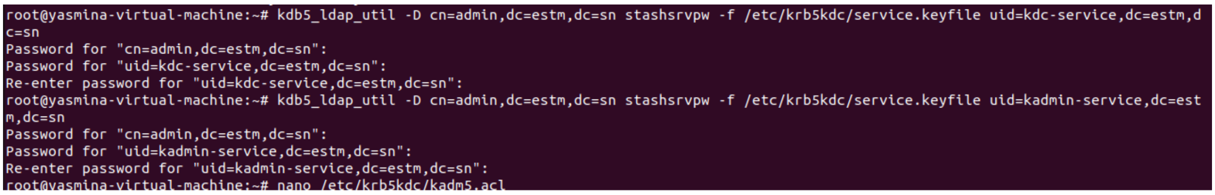
```
[dbdefaults]
ldap_kerberos_container_dn = cn=krbContainer,dc=estm,dc=sn

[dbmodules]
openldap_ldapconf = {
    db_library = kldap
    # if either of these is false, then the ldap_kdc_dn needs to
    # have write access
    disable_last_success = true
    disable_lockout = true
    # this object needs to have read rights on
    # the realm container, principal container and realm sub-trees
    ldap_kdc_dn = "uid=kdc-service,dc=estm,dc=sn"
    # this object needs to have read and write rights on
    # the realm container, principal container and realm sub-trees
    ldap_kadmind_dn = "uid=kadmin-service,dc=estm,dc=sn"
    ldap_service_password_file = /etc/krb5kdc/service.keyfile
    ldap_servers = ldapi:///
    ldap_conns_per_server = 5
}
```

- On utilise l’utilitaire kdb5_ldap_util pour créer le domaine



```
root@yasmina-virtual-machine:~# kdb5_ldap_util -D cn=admin,dc=estm,dc=sn create -subtrees dc=estm,dc=sn -r ESTM.SN -s -H ldapi:///
Password for "cn=admin,dc=estm,dc=sn":
Initializing database for realm 'ESTM.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@yasmina-virtual-machine:~# kdb5_ldap_util -D cn=admin,dc=estm,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile uid=kdc-service,
```

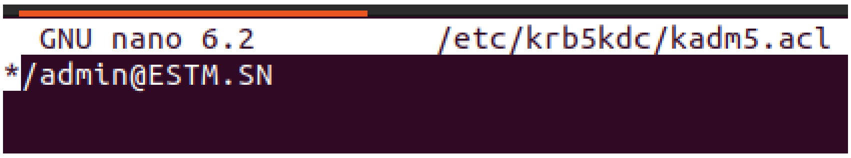
- On crée une réserve du mot de passe utilisé pour la liaison au serveur LDAP. On l’exécute une fois pour chaque ldap_kdc_dn et ldap_kadmin_dn.



```
root@yasmina-virtual-machine:~# kdb5_ldap_util -D cn=admin,dc=estm,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile uid=kdc-service,dc=estm,d
c=sn
Password for "cn=admin,dc=estm,dc=sn":
Password for "uid=kdc-service,dc=estm,dc=sn":
Re-enter password for "uid=kdc-service,dc=estm,dc=sn":
root@yasmina-virtual-machine:~# kdb5_ldap_util -D cn=admin,dc=estm,dc=sn stashsrvpw -f /etc/krb5kdc/service.keyfile uid=kadmin-service,dc=est
m,dc=sn
Password for "cn=admin,dc=estm,dc=sn":
Password for "uid=kadmin-service,dc=estm,dc=sn":
Re-enter password for "uid=kadmin-service,dc=estm,dc=sn":
root@yasmina-virtual-machine:~# nano /etc/krb5kdc/kadm5.acl
```

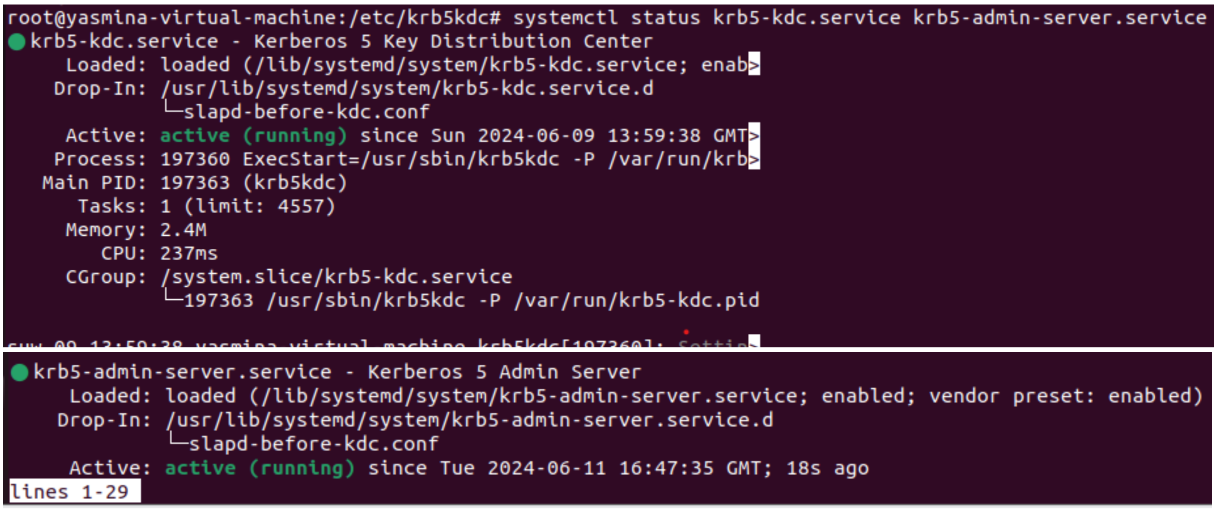
Le fichier contient maintenant des versions en texte clair des mots de passe utilisés par le KDC pour contacter le serveur LDAP /etc/krb5kdc/service.keyfile.

- Créons un fichier /etc/krb5kdc/kadm5.acl pour le serveur d'administration



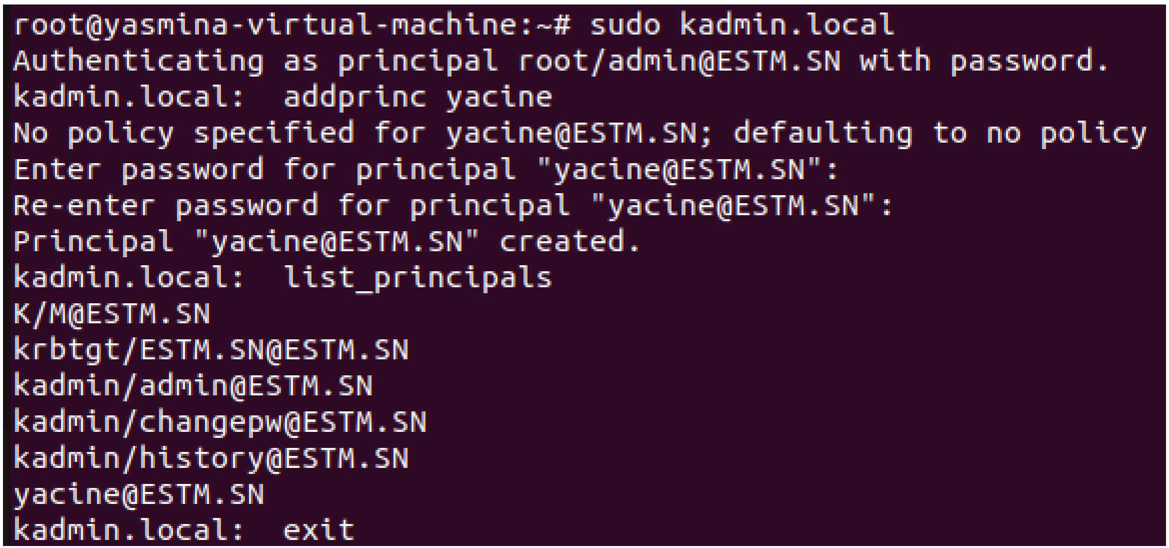
```
  GNU nano 6.2            /etc/krb5kdc/kadm5.acl
*/admin@ESTM.SN
```

- On redémarre le KDC Kerberos et le serveur d’administration



```
root@yasmina-virtual-machine:/etc/krb5kdc# systemctl status krb5-kdc.service krb5-admin-server.service
● krb5-kdc.service - Kerberos 5 Key Distribution Center
     Loaded: loaded (/lib/systemd/system/krb5-kdc.service; enab>
    Drop-In: /usr/lib/systemd/system/krb5-kdc.service.d
             └─slapd-before-kdc.conf
     Active: active (running) since Sun 2024-06-09 13:59:38 GMT>
    Process: 197360 ExecStart=/usr/sbin/krb5kdc -P /var/run/krb>
   Main PID: 197363 (krb5kdc)
      Tasks: 1 (limit: 4557)
     Memory: 2.4M
        CPU: 237ms
     CGroup: /system.slice/krb5-kdc.service
             └─197363 /usr/sbin/krb5kdc -P /var/run/krb5-kdc.pid

juin 09 13:59:38 yasmina-virtual-machine krb5kdc[197360]: Settin>
● krb5-admin-server.service - Kerberos 5 Admin Server
     Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)
    Drop-In: /usr/lib/systemd/system/krb5-admin-server.service.d
             └─slapd-before-kdc.conf
     Active: active (running) since Tue 2024-06-11 16:47:35 GMT; 18s ago
lines 1-29
```

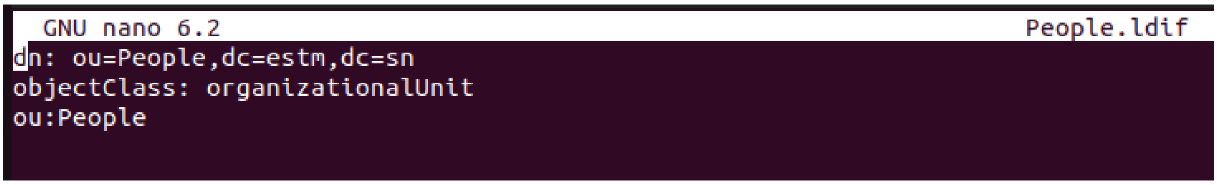
- Nous pouvons désormais ajouter des principaux Kerberos à la base de données LDAP et ils seront copiés sur tout autre serveur LDAP configuré pour la réplication.



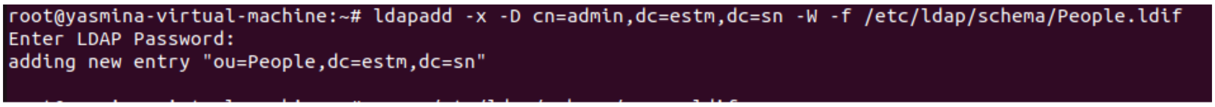
```
root@yasmina-virtual-machine:~# sudo kadmin.local
Authenticating as principal root/admin@ESTM.SN with password.
kadmin.local:  addprinc yacine
No policy specified for yacine@ESTM.SN; defaulting to no policy
Enter password for principal "yacine@ESTM.SN":
Re-enter password for principal "yacine@ESTM.SN":
Principal "yacine@ESTM.SN" created.
kadmin.local:  list_principals
K/M@ESTM.SN
krbtgt/ESTM.SN@ESTM.SN
kadmin/admin@ESTM.SN
kadmin/changepw@ESTM.SN
kadmin/history@ESTM.SN
yacine@ESTM.SN
kadmin.local:  exit
```

- Et maintenant, nous pouvons spécifier le principal.

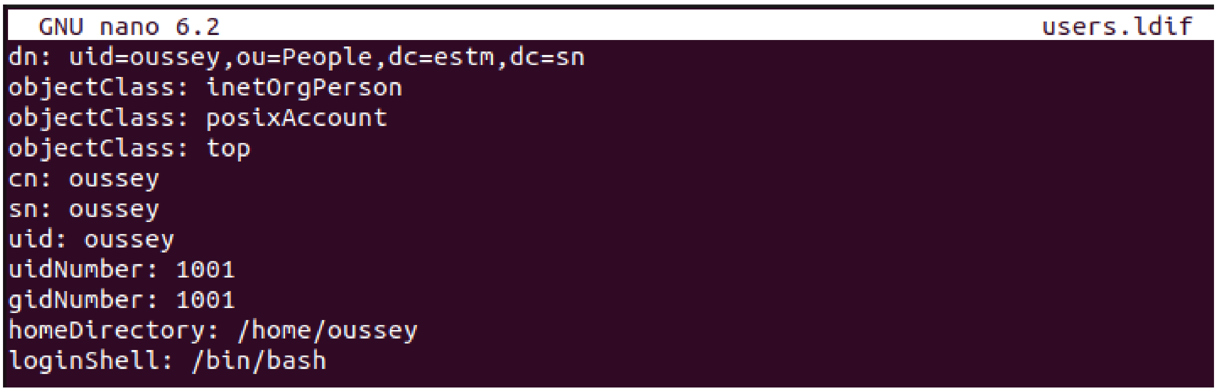
  Avant cela on crée un utilisateur dans LDAP



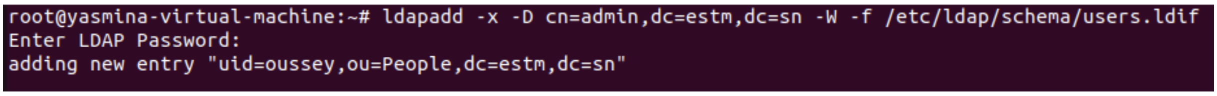
```
  GNU nano 6.2                                                    People.ldif
dn: ou=People,dc=estm,dc=sn
objectClass: organizationalUnit
ou:People
```



```
root@yasmina-virtual-machine:~# ldapadd -x -D cn=admin,dc=estm,dc=sn -W -f /etc/ldap/schema/People.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=estm,dc=sn"
```

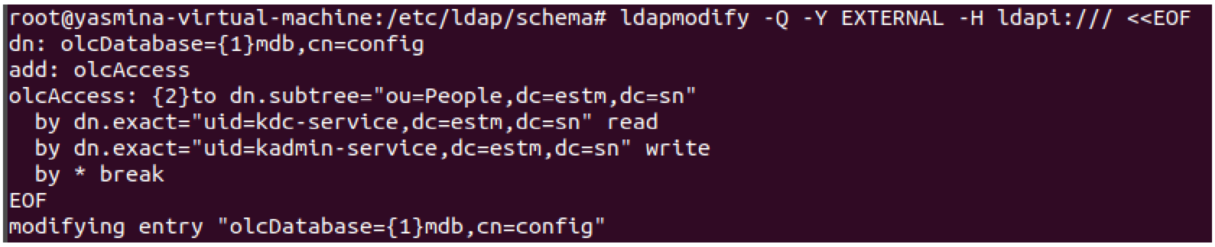


```
  GNU nano 6.2                                                     users.ldif
dn: uid=oussey,ou=People,dc=estm,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
cn: oussey
sn: oussey
uid: oussey
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/oussey
loginShell: /bin/bash
```



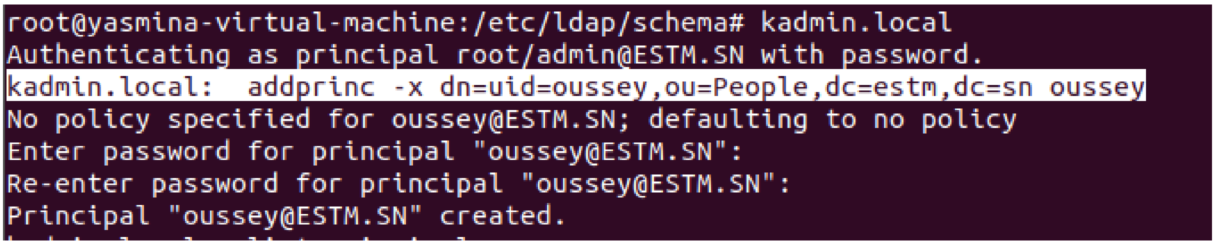
```
root@yasmina-virtual-machine:~# ldapadd -x -D cn=admin,dc=estm,dc=sn -W -f /etc/ldap/schema/users.ldif
Enter LDAP Password:
adding new entry "uid=oussey,ou=People,dc=estm,dc=sn"
```

- Mettons à jour les ACL

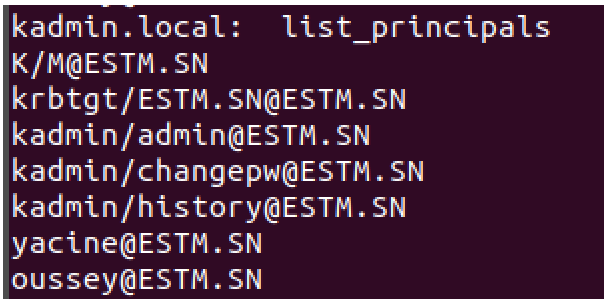


```
root@yasmina-virtual-machine:/etc/ldap/schema# ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF
dn: olcDatabase={1}mdb,cn=config
add: olcAccess
olcAccess: {2}to dn.subtree="ou=People,dc=estm,dc=sn"
  by dn.exact="uid=kdc-service,dc=estm,dc=sn" read
  by dn.exact="uid=kadmin-service,dc=estm,dc=sn" write
  by * break
EOF
modifying entry "olcDatabase={1}mdb,cn=config"
```

- Et maintenant on ajoute des utilisateurs sur kerberos qui va se stocker dans ldap



```
root@yasmina-virtual-machine:/etc/ldap/schema# kadmin.local
Authenticating as principal root/admin@ESTM.SN with password.
kadmin.local:  addprinc -x dn=uid=oussey,ou=People,dc=estm,dc=sn oussey
No policy specified for oussey@ESTM.SN; defaulting to no policy
Enter password for principal "oussey@ESTM.SN":
Re-enter password for principal "oussey@ESTM.SN":
Principal "oussey@ESTM.SN" created.
```

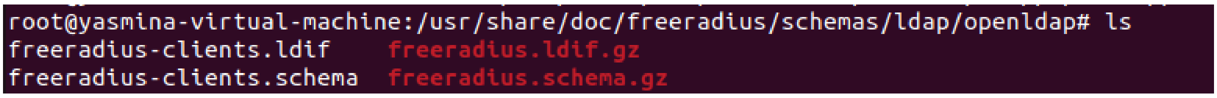


```
kadmin.local:  list_principals
K/M@ESTM.SN
krbtgt/ESTM.SN@ESTM.SN
kadmin/admin@ESTM.SN
kadmin/changepw@ESTM.SN
kadmin/history@ESTM.SN
yacine@ESTM.SN
oussey@ESTM.SN
```

4. Configuration de LDAP pour freeradius

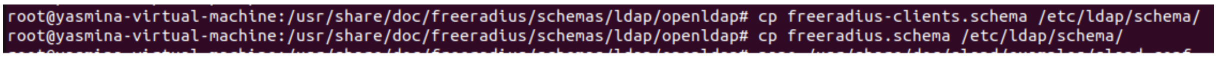
a) Configuration du serveur

- On se déplace dans le dossier /usr/share/doc/freeradius/schemas/ldap/openldap



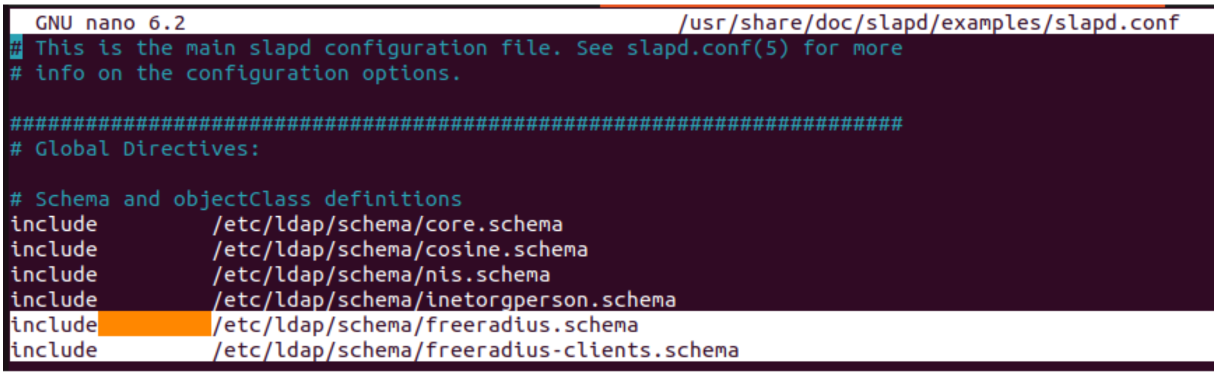
```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# ls
freeradius-clients.ldif    freeradius.ldif.gz
freeradius-clients.schema  freeradius.schema.gz
```

- On copie freeradius-clients.schema et freeradius.schema dans /etc/ldap/schema/

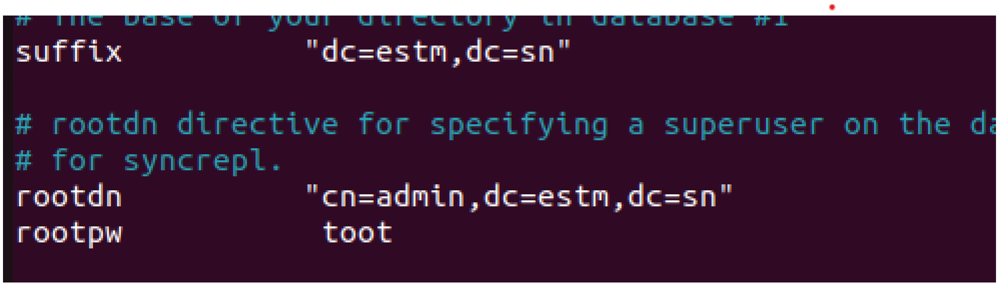


```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# cp freeradius-clients.schema /etc/ldap/schema/
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# cp freeradius.schema /etc/ldap/schema/
```

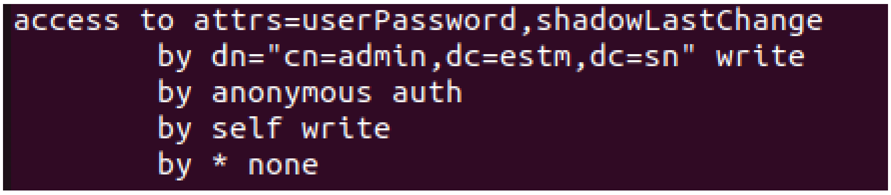
- On édite le fichier slapd.conf pour importer les schémas en ajoutant les deux dernières lignes et les configuration ci-dessous



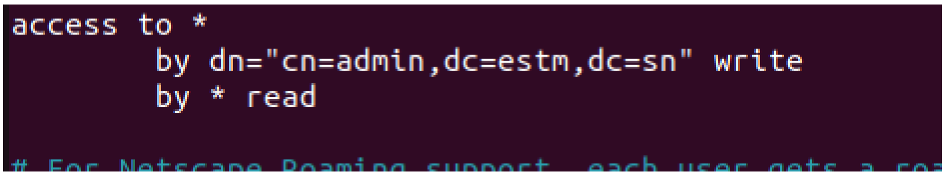
```
  GNU nano 6.2                                     /usr/share/doc/slapd/examples/slapd.conf
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

#######################################################################
# Global Directives:

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/freeradius.schema
include         /etc/ldap/schema/freeradius-clients.schema
```



```
# The base of your directory in database #1
suffix          "dc=estm,dc=sn"

# rootdn directive for specifying a superuser on the da
# for syncrepl.
rootdn          "cn=admin,dc=estm,dc=sn"
rootpw           toot
```



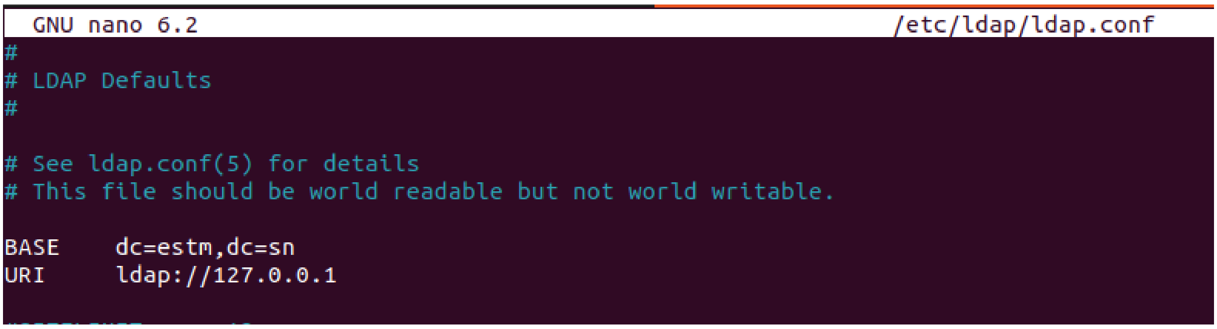
```
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=estm,dc=sn" write
        by anonymous auth
        by self write
        by * none
```



```
access to *
        by dn="cn=admin,dc=estm,dc=sn" write
        by * read

# For Netscape Roaming support, each user gets a roa
```

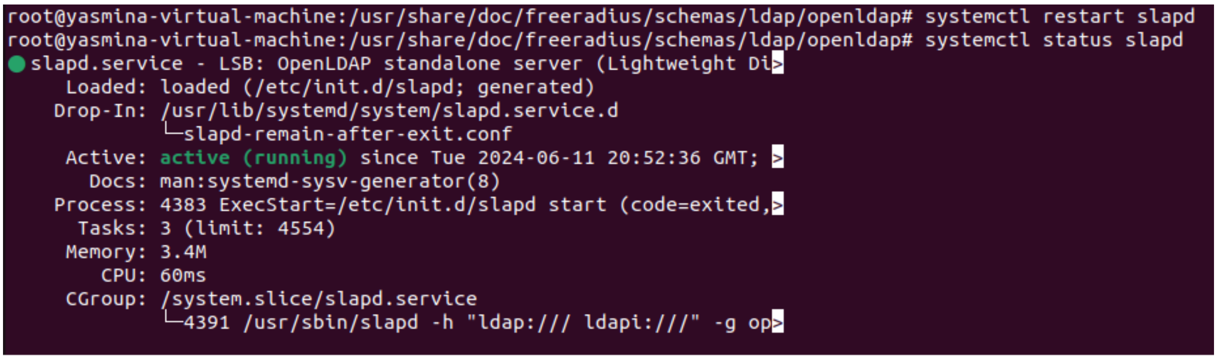
a) **Configuration du client**

- Cela se passe dans le fichier /etc/ldap/ldap.conf



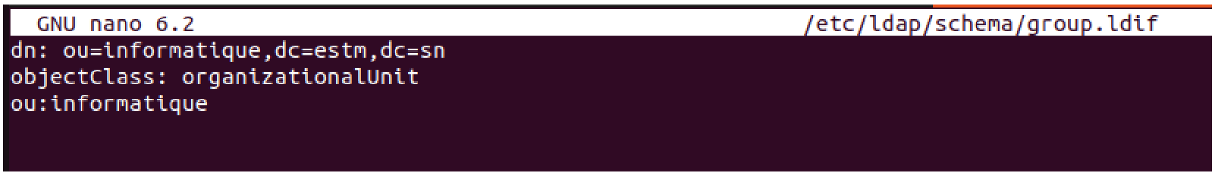
```
  GNU nano 6.2                                                /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=estm,dc=sn
URI     ldap://127.0.0.1
```

- Par la suite, on redémarre le service



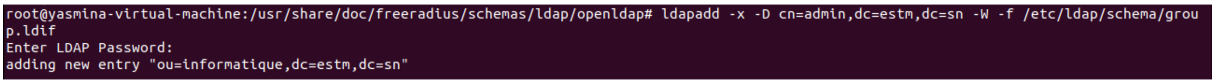
```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# systemctl restart slapd
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Di>
     Loaded: loaded (/etc/init.d/slapd; generated)
    Drop-In: /usr/lib/systemd/system/slapd.service.d
             └─slapd-remain-after-exit.conf
     Active: active (running) since Tue 2024-06-11 20:52:36 GMT; >
       Docs: man:systemd-sysv-generator(8)
    Process: 4383 ExecStart=/etc/init.d/slapd start (code=exited,>
      Tasks: 3 (limit: 4554)
     Memory: 3.4M
        CPU: 60ms
     CGroup: /system.slice/slapd.service
             └─4391 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g op>
```

- On crée un fichier group.ldif dans le schéma pour pouvoir créer des groupes



```
  GNU nano 6.2                                      /etc/ldap/schema/group.ldif
dn: ou=informatique,dc=estm,dc=sn
objectClass: organizationalUnit
ou:informatique
```

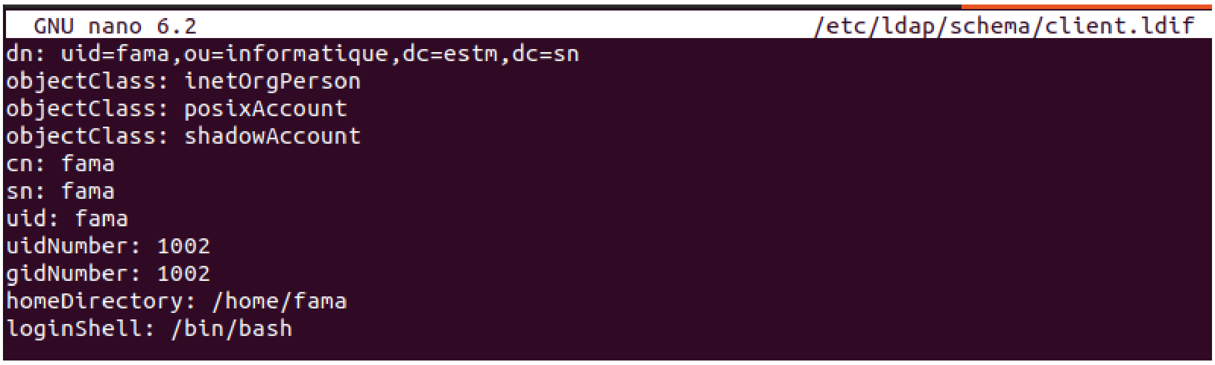
- On ajoute le fichier group.ldif dans l’annuaire



```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# ldapadd -x -D cn=admin,dc=estm,dc=sn -W -f /etc/ldap/schema/grou
p.ldif
Enter LDAP Password:
adding new entry "ou=informatique,dc=estm,dc=sn"
```

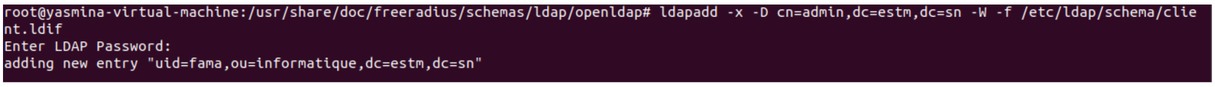
- Insérons un utilisateur dans notre annuaire en le mettant dans le groupe

- On ajoute le fichier group.ldif dans l’annuaire



```
  GNU nano 6.2                                          /etc/ldap/schema/client.ldif
dn: uid=fama,ou=informatique,dc=estm,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: fama
sn: fama
uid: fama
uidNumber: 1002
gidNumber: 1002
homeDirectory: /home/fama
loginShell: /bin/bash
```

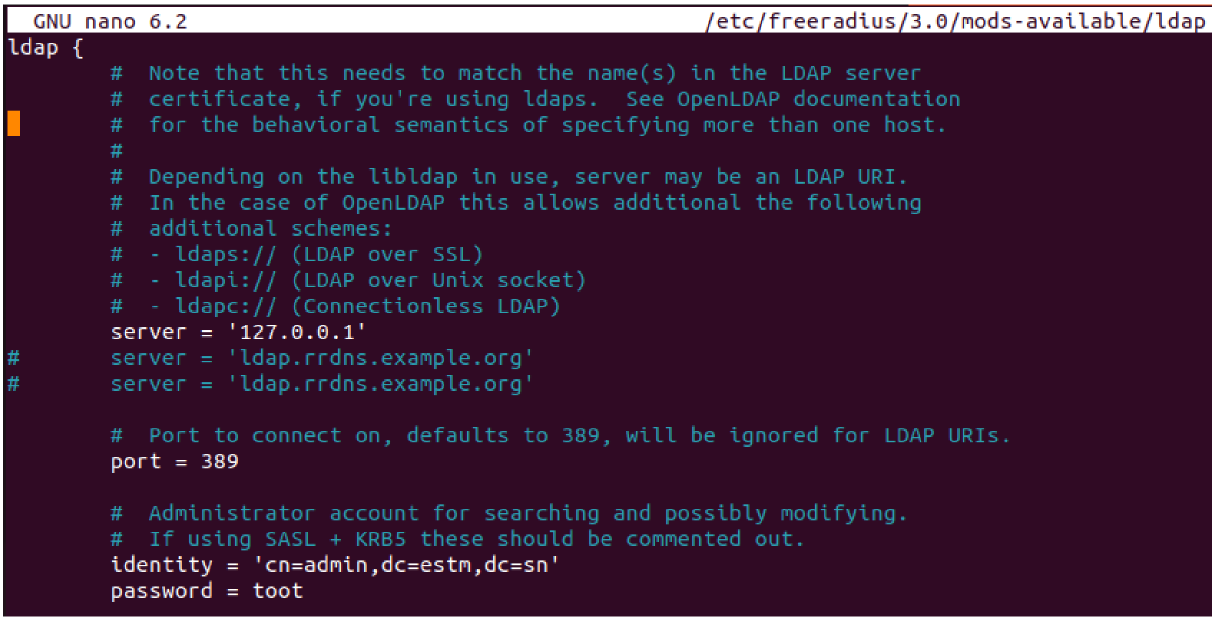
- On ajoute le fichier group.ldif dans l'annuaire



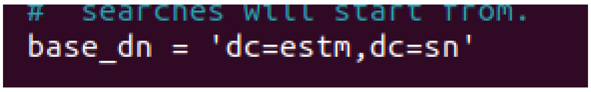
```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# ldapadd -x -D cn=admin,dc=estm,dc=sn -W -f /etc/ldap/schema/clie
nt.ldif
Enter LDAP Password:
adding new entry "uid=fama,ou=informatique,dc=estm,dc=sn"
```

1. **Configuration de freeradius et Ldap**

- On donne les paramètres de connexion de l'annuaire à freeradius dans le fichier /etc/freeradius/3.0/mods-available/ldap

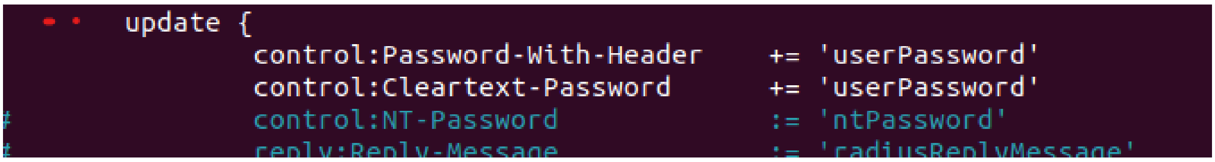


```
  GNU nano 6.2                              /etc/freeradius/3.0/mods-available/ldap
ldap {
        #  Note that this needs to match the name(s) in the LDAP server
        #  certificate, if you're using ldaps.  See OpenLDAP documentation
        #  for the behavioral semantics of specifying more than one host.
        #
        #  Depending on the libldap in use, server may be an LDAP URI.
        #  In the case of OpenLDAP this allows additional the following
        #  additional schemes:
        #  - ldaps:// (LDAP over SSL)
        #  - ldapi:// (LDAP over Unix socket)
        #  - ldapc:// (Connectionless LDAP)
        server = '127.0.0.1'
#       server = 'ldap.rrdns.example.org'
#       server = 'ldap.rrdns.example.org'

        #  Port to connect on, defaults to 389, will be ignored for LDAP URIs.
        port = 389

        #  Administrator account for searching and possibly modifying.
        #  If using SASL + KRB5 these should be commented out.
        identity = 'cn=admin,dc=estm,dc=sn'
        password = toot
```



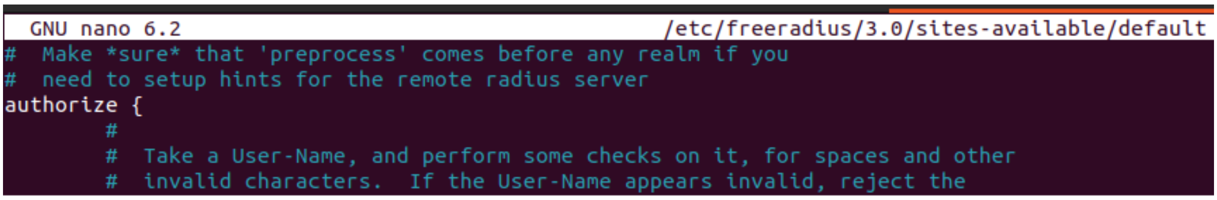
```
  #  searches will start from.
  base_dn = 'dc=estm,dc=sn'
```

- On fait le mapping entre les attributs radius et ldap en ajoutant la ligne suivante control:Cleartext-Password += 'userPassword' dans la rubrique update

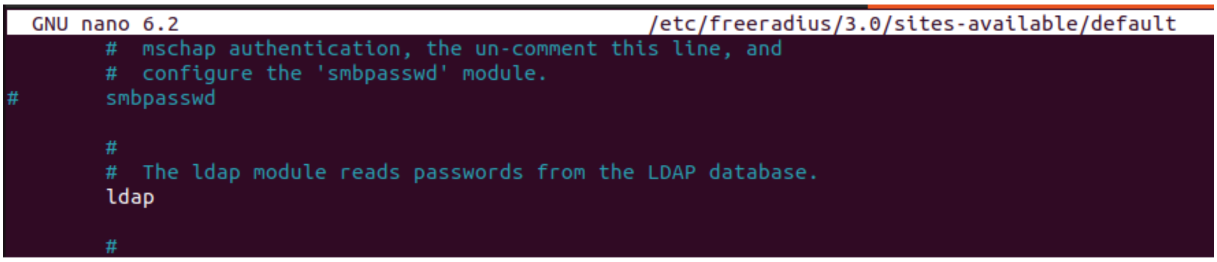


```
        update {
                control:Password-With-Header    += 'userPassword'
                control:Cleartext-Password      += 'userPassword'
#               control:NT-Password             := 'ntPassword'
#               reply:Reply-Message             := 'radiusReplyMessage'
```

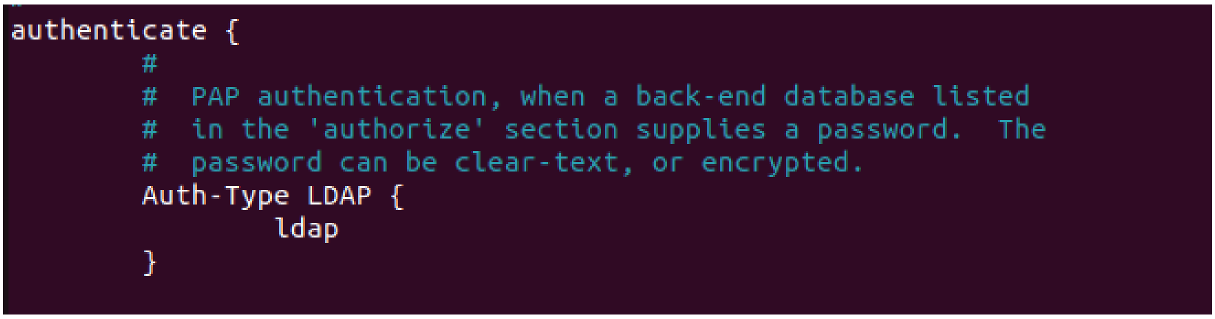
- Ensuite dans le fichier /etc/freeradius/3.0/sites-available/default, on enlève le « -» devant LDAP dans la section authorize



```
  GNU nano 6.2                          /etc/freeradius/3.0/sites-available/default
#  Make *sure* that 'preprocess' comes before any realm if you
#  need to setup hints for the remote radius server
authorize {
        #
        #  Take a User-Name, and perform some checks on it, for spaces and other
        #  invalid characters.  If the User-Name appears invalid, reject the
```

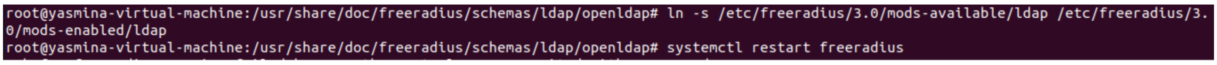


```
  GNU nano 6.2                          /etc/freeradius/3.0/sites-available/default
        #  mschap authentication, the un-comment this line, and
        #  configure the 'smbpasswd' module.
#       smbpasswd

        #
        #  The ldap module reads passwords from the LDAP database.
        ldap

        #
```



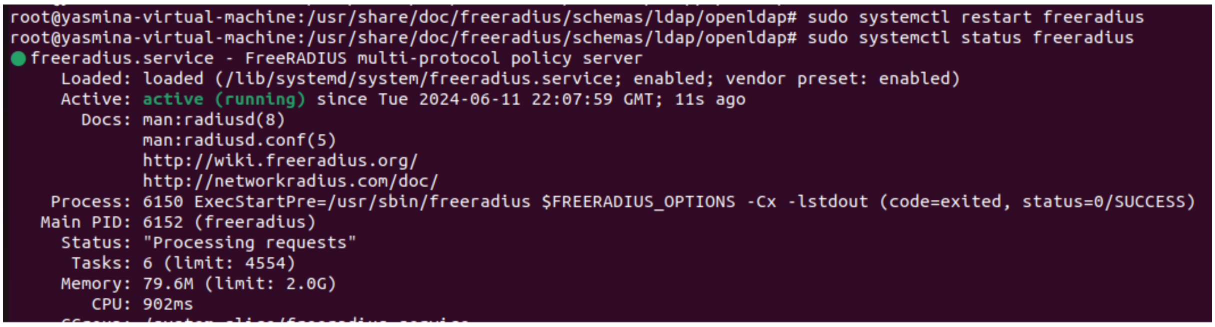
```
authenticate {
        #
        #  PAP authentication, when a back-end database listed
        #  in the 'authorize' section supplies a password.  The
        #  password can be clear-text, or encrypted.
        Auth-Type LDAP {
                ldap
        }
```

- On crée un lien symbolique



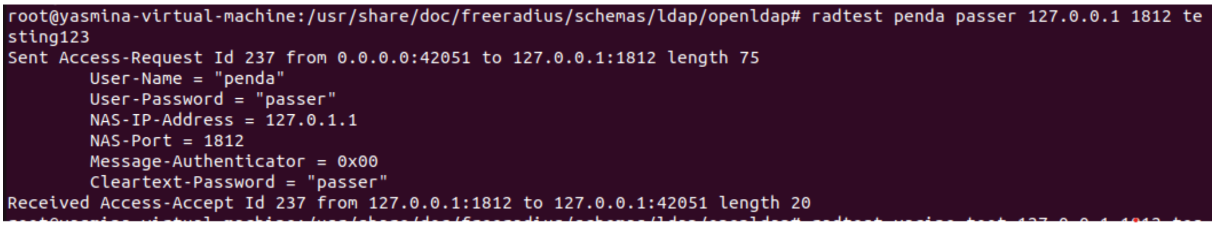
```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# ln -s /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled/ldap
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# systemctl restart freeradius
```

- On redémarre freeradius



```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# sudo systemctl restart freeradius
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# sudo systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-06-11 22:07:59 GMT; 11s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
    Process: 6150 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited, status=0/SUCCESS)
   Main PID: 6152 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 4554)
     Memory: 79.6M (limit: 2.0G)
        CPU: 902ms
```

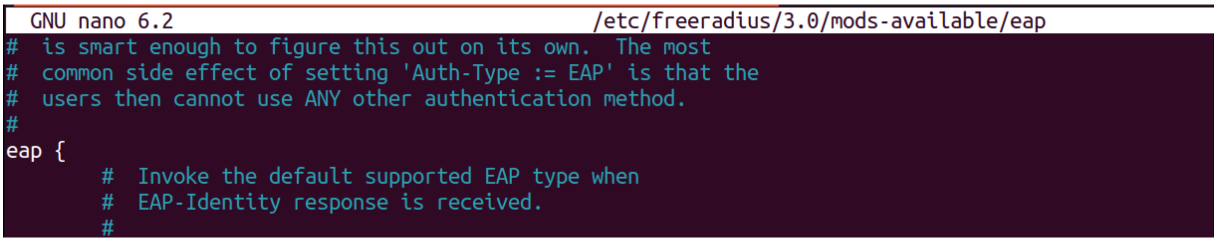
Test



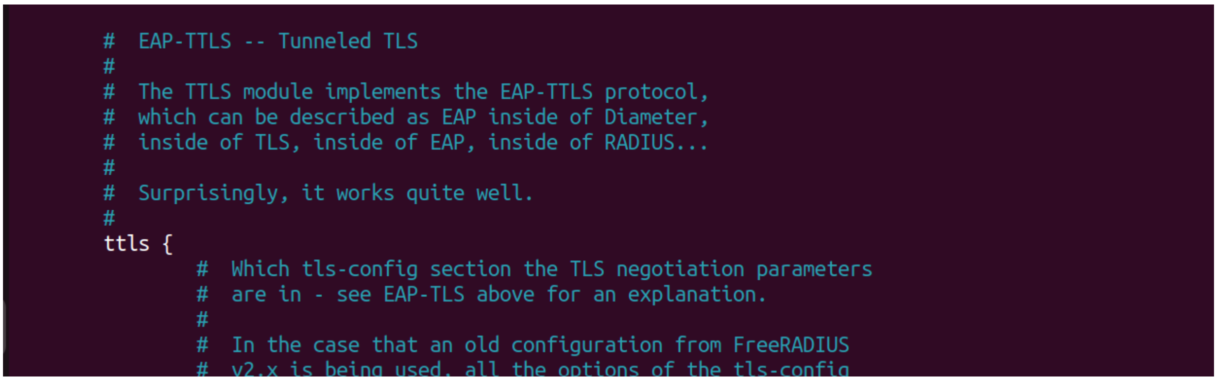
```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# radtest penda passer 127.0.0.1 1812 te
sting123
Sent Access-Request Id 237 from 0.0.0.0:42051 to 127.0.0.1:1812 length 75
        User-Name = "penda"
        User-Password = "passer"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 1812
        Message-Authenticator = 0x00
        Cleartext-Password = "passer"
Received Access-Accept Id 237 from 127.0.0.1:1812 to 127.0.0.1:42051 length 20
```

1) Méthodes d'authentification EAP-TTLS

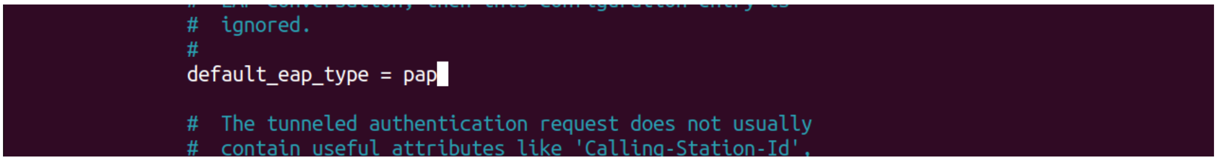
Activons TTLS dans le fichier /etc/freeradius/3.0/mods-available/eap



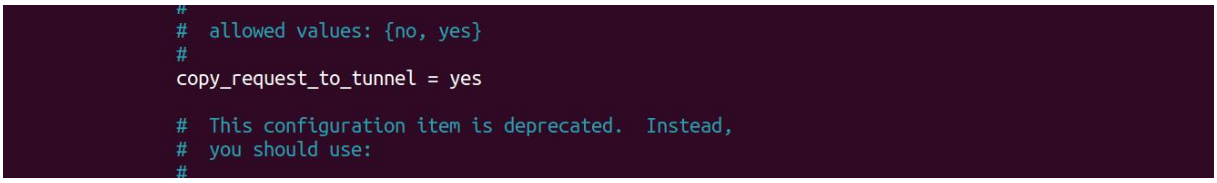
```
  GNU nano 6.2                                  /etc/freeradius/3.0/mods-available/eap
#  is smart enough to figure this out on its own.  The most
#  common side effect of setting 'Auth-Type := EAP' is that the
#  users then cannot use ANY other authentication method.
#
eap {
        #  Invoke the default supported EAP type when
        #  EAP-Identity response is received.
        #
```



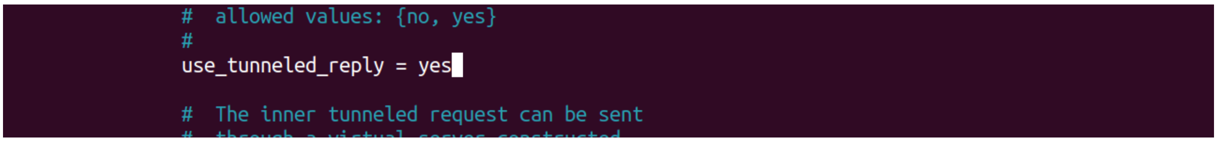
```
        #  EAP-TTLS -- Tunneled TLS
        #
        #  The TTLS module implements the EAP-TTLS protocol,
        #  which can be described as EAP inside of Diameter,
        #  inside of TLS, inside of EAP, inside of RADIUS...
        #
        #  Surprisingly, it works quite well.
        #
        ttls {
                #  Which tls-config section the TLS negotiation parameters
                #  are in - see EAP-TLS above for an explanation.
                #
                #  In the case that an old configuration from FreeRADIUS
                #  v2.x is being used, all the options of the tls-config
```



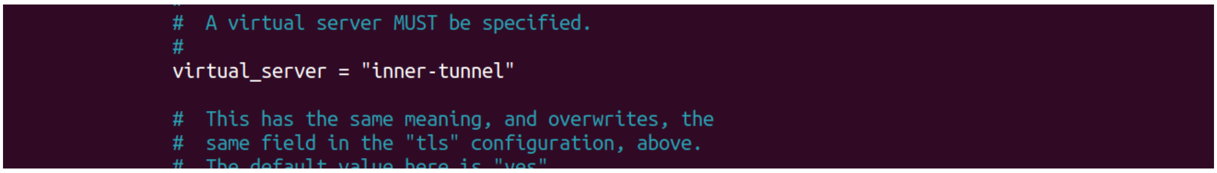
```
                #  EAP conversation, then this configuration entry is
                #  ignored.
                #
                default_eap_type = pap

                #  The tunneled authentication request does not usually
                #  contain useful attributes like 'Calling-Station-Id',
```



```
                #
                #  allowed values: {no, yes}
                #
                copy_request_to_tunnel = yes

                #  This configuration item is deprecated.  Instead,
                #  you should use:
                #
```

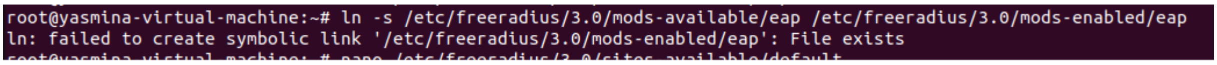


```
                #  allowed values: {no, yes}
                #
                use_tunneled_reply = yes

                #  The inner tunneled request can be sent
                #  through a virtual server constructed
```



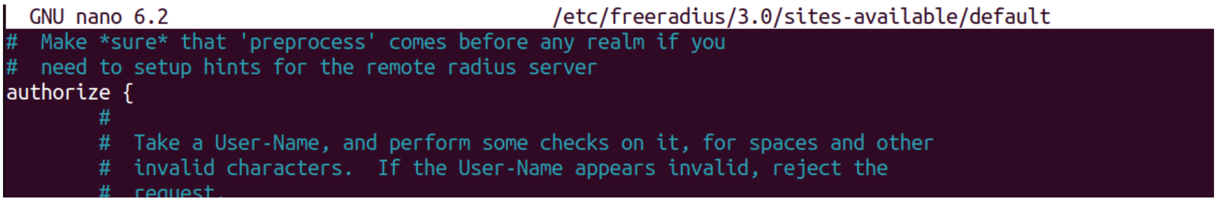
```
               #  A virtual server MUST be specified.
               #
               virtual_server = "inner-tunnel"

               #  This has the same meaning, and overwrites, the
               #  same field in the "tls" configuration, above.
               #  The default value here is "yes".
```

Créons un lien symbolique pour activer le module EAP

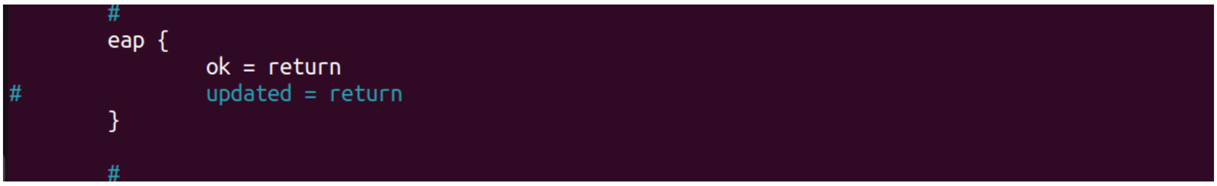


```
root@yasmina-virtual-machine:~# ln -s /etc/freeradius/3.0/mods-available/eap /etc/freeradius/3.0/mods-enabled/eap
ln: failed to create symbolic link '/etc/freeradius/3.0/mods-enabled/eap': File exists
root@yasmina-virtual-machine:~# nano /etc/freeradius/3.0/sites-available/default
```

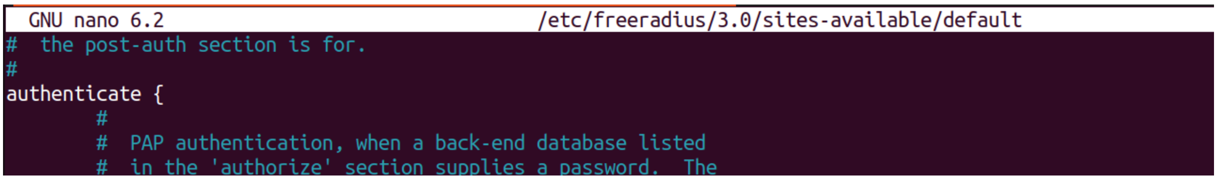
Configurons le serveur virtuel



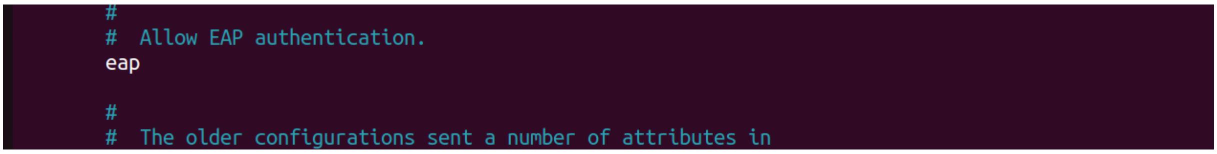
```
  GNU nano 6.2                                /etc/freeradius/3.0/sites-available/default
#  Make *sure* that 'preprocess' comes before any realm if you
#  need to setup hints for the remote radius server
authorize {
        #
        #  Take a User-Name, and perform some checks on it, for spaces and other
        #  invalid characters.  If the User-Name appears invalid, reject the
        #  request.
```



```
        #
        eap {
                ok = return
#               updated = return
        }

        #
```

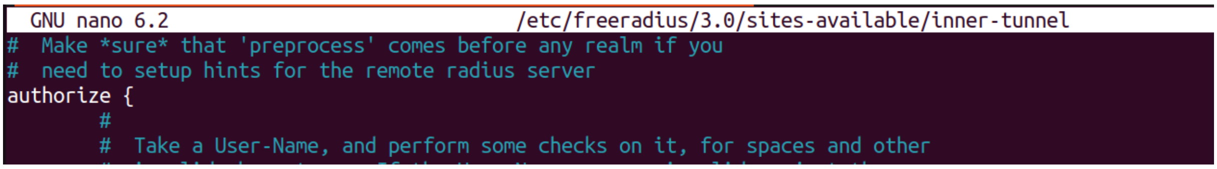


```
  GNU nano 6.2                                /etc/freeradius/3.0/sites-available/default
#  the post-auth section is for.
#
authenticate {
        #
        #  PAP authentication, when a back-end database listed
        #  in the 'authorize' section supplies a password.  The
```

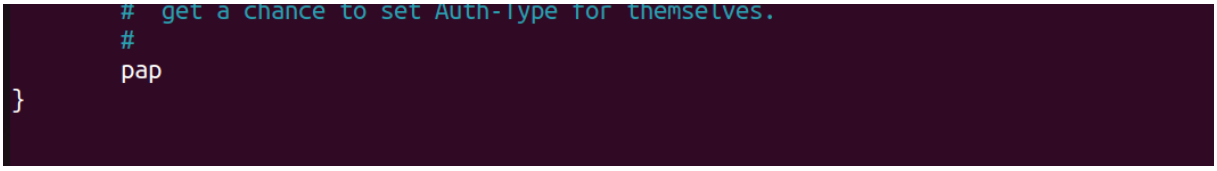


```
        #
        #  Allow EAP authentication.
        eap

        #
        #  The older configurations sent a number of attributes in
```

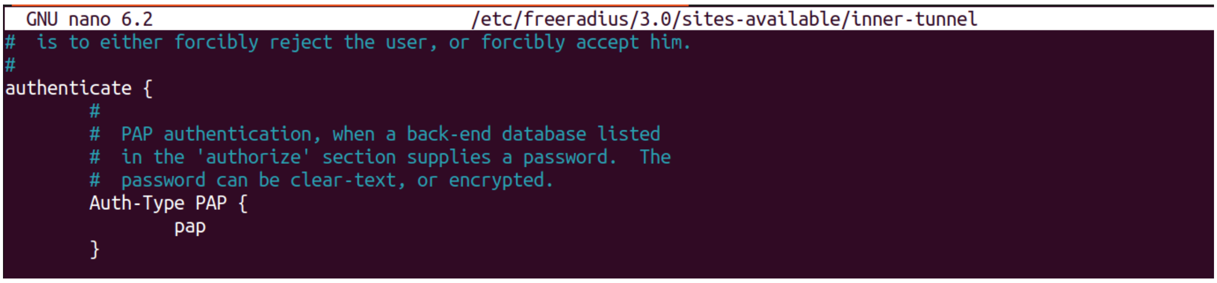
Configurons le serveur virtuel "inner-tunnel"



```
  GNU nano 6.2                                /etc/freeradius/3.0/sites-available/inner-tunnel
#  Make *sure* that 'preprocess' comes before any realm if you
#  need to setup hints for the remote radius server
authorize {
        #
        #  Take a User-Name, and perform some checks on it, for spaces and other
        #  invalid characters.  If the User-Name appears invalid, reject the
```

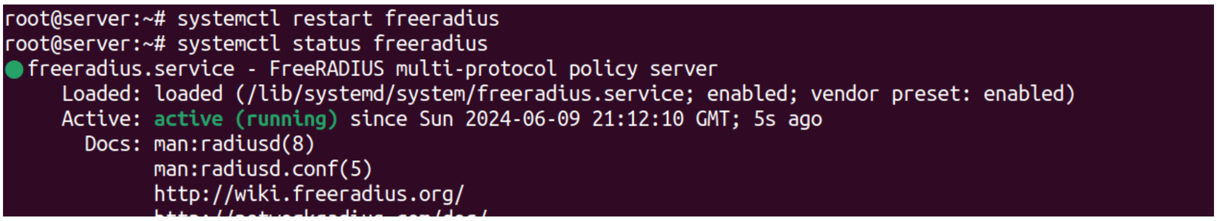


```
        #  get a chance to set Auth-Type for themselves.
        #
        pap
}
```



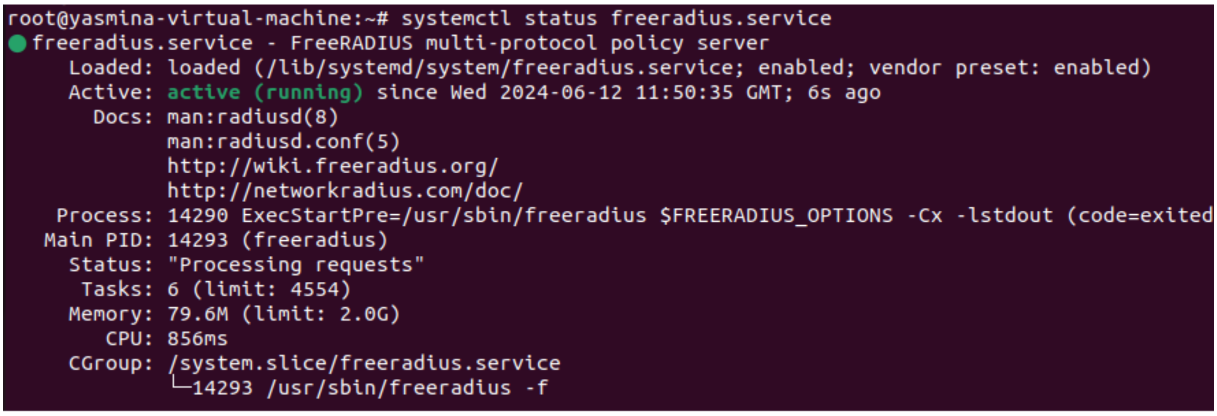
```
  GNU nano 6.2                                   /etc/freeradius/3.0/sites-available/inner-tunnel
#  is to either forcibly reject the user, or forcibly accept him.
#
authenticate {
        #
        #  PAP authentication, when a back-end database listed
        #  in the 'authorize' section supplies a password.  The
        #  password can be clear-text, or encrypted.
        Auth-Type PAP {
                pap
        }
```

Redémarrons FreeRADIUS

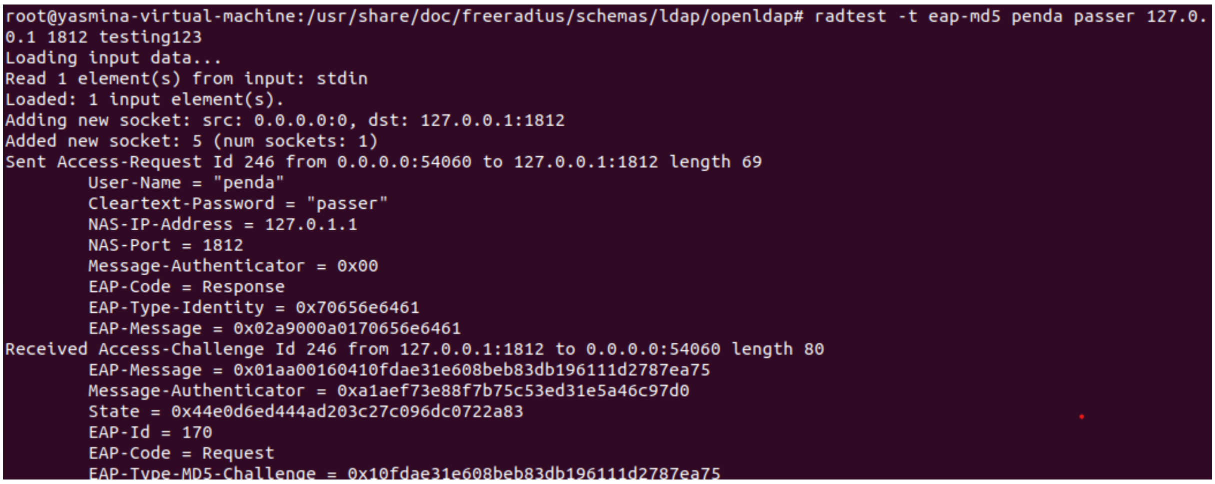


```
root@server:~# systemctl restart freeradius
root@server:~# systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2024-06-09 21:12:10 GMT; 5s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
```

Testons l'authentification EAP-TTLS



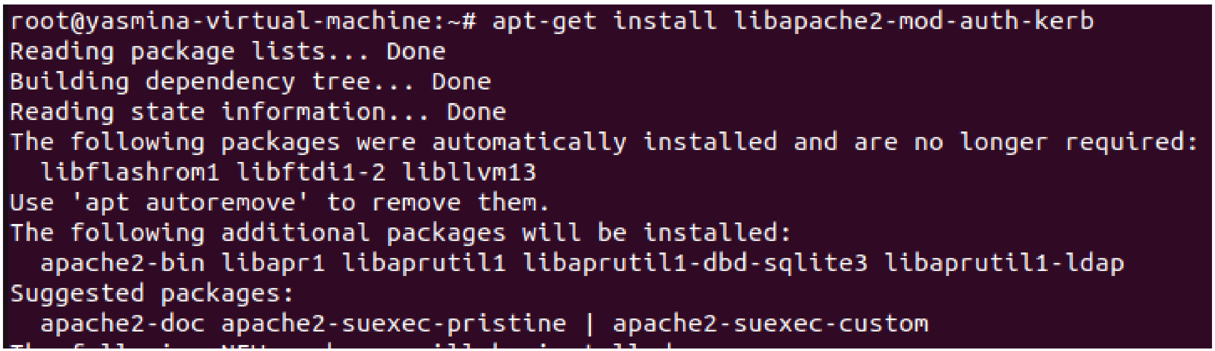
```
root@yasmina-virtual-machine:~# systemctl status freeradius.service
● freeradius.service - FreeRADIUS multi-protocol policy server
     Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-06-12 11:50:35 GMT; 6s ago
       Docs: man:radiusd(8)
             man:radiusd.conf(5)
             http://wiki.freeradius.org/
             http://networkradius.com/doc/
    Process: 14290 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cx -lstdout (code=exited
   Main PID: 14293 (freeradius)
     Status: "Processing requests"
      Tasks: 6 (limit: 4554)
     Memory: 79.6M (limit: 2.0G)
        CPU: 856ms
     CGroup: /system.slice/freeradius.service
             └─14293 /usr/sbin/freeradius -f
```



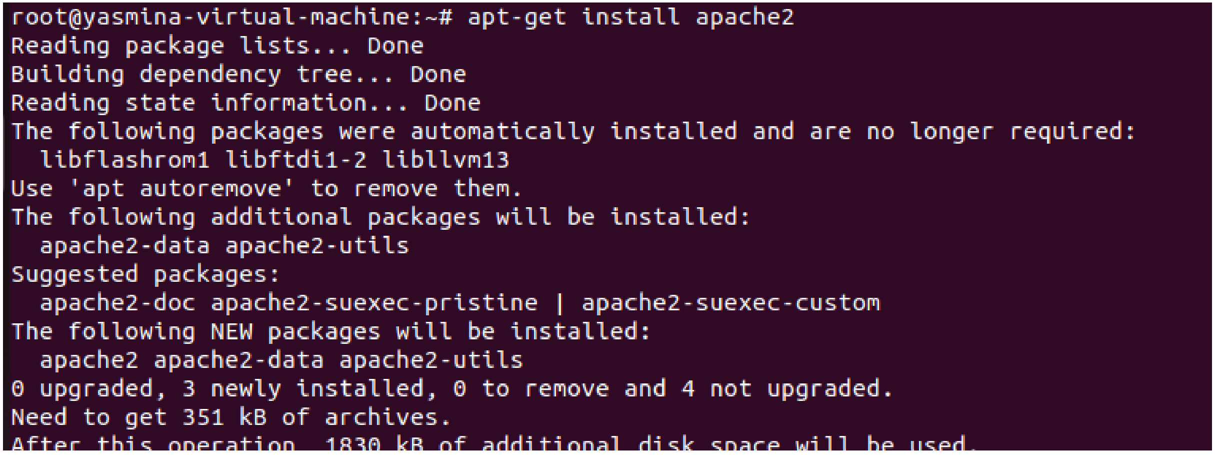
```
root@yasmina-virtual-machine:/usr/share/doc/freeradius/schemas/ldap/openldap# radtest -t eap-md5 penda passer 127.0.
0.1 1812 testing123
Loading input data...
Read 1 element(s) from input: stdin
Loaded: 1 input element(s).
Adding new socket: src: 0.0.0.0:0, dst: 127.0.0.1:1812
Added new socket: 5 (num sockets: 1)
Sent Access-Request Id 246 from 0.0.0.0:54060 to 127.0.0.1:1812 length 69
        User-Name = "penda"
        Cleartext-Password = "passer"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 1812
        Message-Authenticator = 0x00
        EAP-Code = Response
        EAP-Type-Identity = 0x70656e6461
        EAP-Message = 0x02a9000a0170656e6461
Received Access-Challenge Id 246 from 127.0.0.1:1812 to 0.0.0.0:54060 length 80
        EAP-Message = 0x01aa00160410fdae31e608beb83db196111d2787ea75
        Message-Authenticator = 0xa1aef73e88f7b75c53ed31e5a46c97d0
        State = 0x44e0d6ed444ad203c27c096dc0722a83
        EAP-Id = 170
        EAP-Code = Request
        EAP-Type-MD5-Challenge = 0x10fdae31e608beb83db196111d2787ea75
```

1. Configuration de Apache pour utiliser Kerberos

On install ces packets

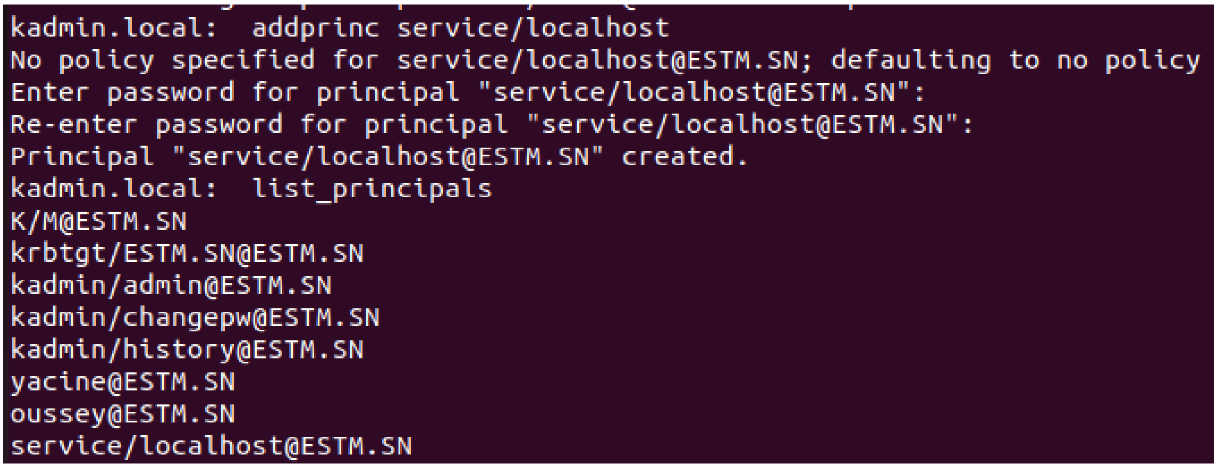


```
root@yasmina-virtual-machine:~# apt-get install libapache2-mod-auth-kerb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libllvm13
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```



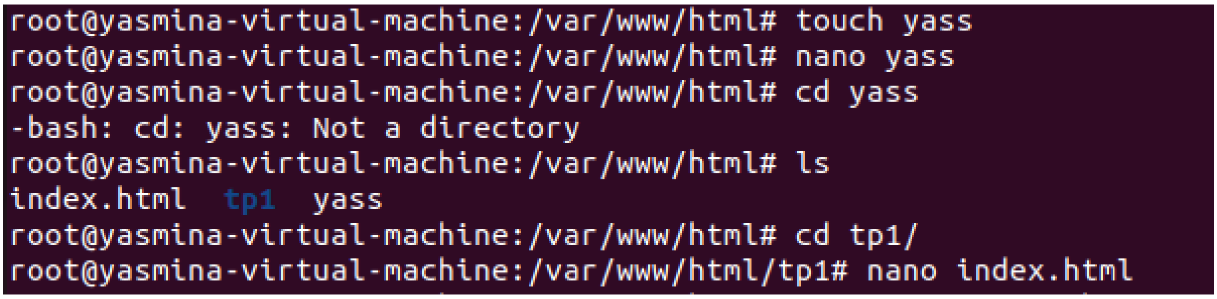
```
root@yasmina-virtual-machine:~# apt-get install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2 libllvm13
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
0 upgraded, 3 newly installed, 0 to remove and 4 not upgraded.
Need to get 351 kB of archives.
After this operation, 1830 kB of additional disk space will be used.
```

- Ensuite on ajoute ce principal pour le server APACHE



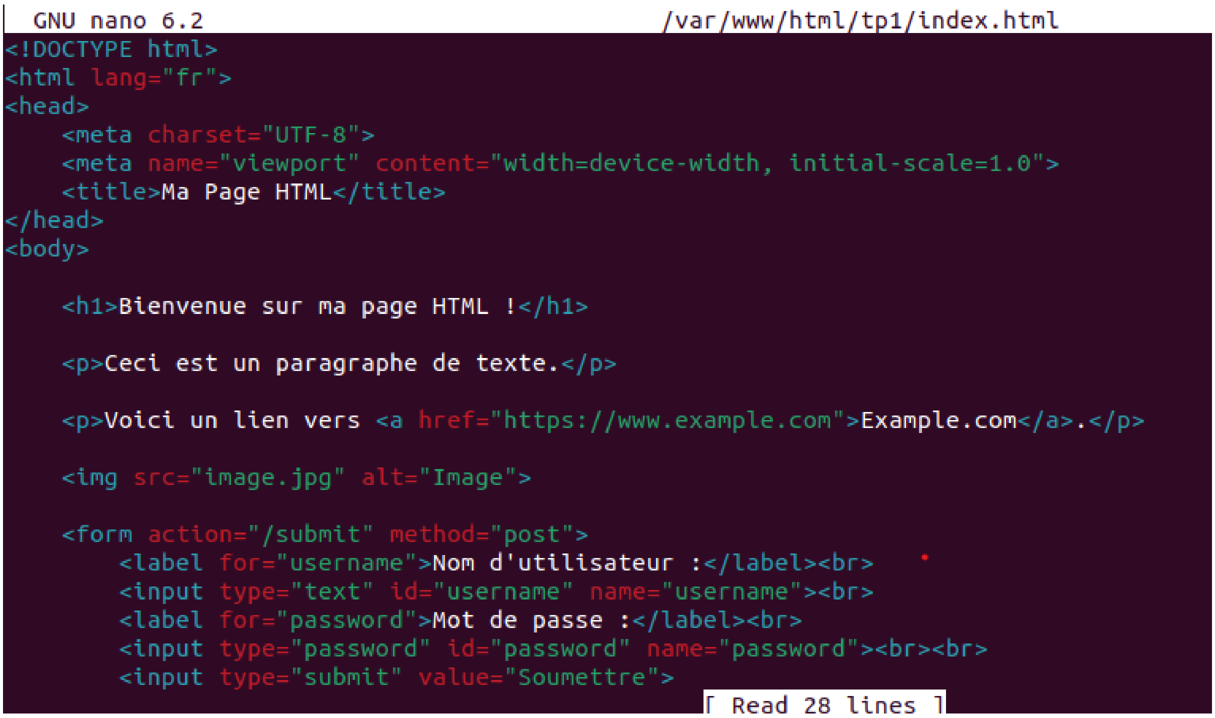
```
kadmin.local:  addprinc service/localhost
No policy specified for service/localhost@ESTM.SN; defaulting to no policy
Enter password for principal "service/localhost@ESTM.SN":
Re-enter password for principal "service/localhost@ESTM.SN":
Principal "service/localhost@ESTM.SN" created.
kadmin.local:  list_principals
K/M@ESTM.SN
krbtgt/ESTM.SN@ESTM.SN
kadmin/admin@ESTM.SN
kadmin/changepw@ESTM.SN
kadmin/history@ESTM.SN
yacine@ESTM.SN
oussey@ESTM.SN
service/localhost@ESTM.SN
```

Ensuite on crée le fichier index.html sur tp1



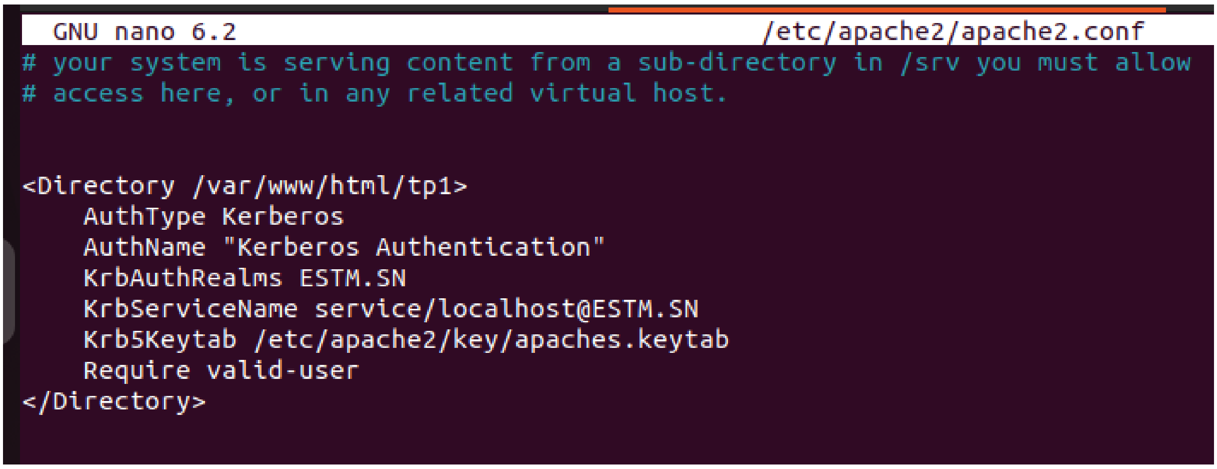
```
root@yasmina-virtual-machine:/var/www/html# touch yass
root@yasmina-virtual-machine:/var/www/html# nano yass
root@yasmina-virtual-machine:/var/www/html# cd yass
-bash: cd: yass: Not a directory
root@yasmina-virtual-machine:/var/www/html# ls
index.html  tp1  yass
root@yasmina-virtual-machine:/var/www/html# cd tp1/
root@yasmina-virtual-machine:/var/www/html/tp1# nano index.html
```

Ensuite on met ce code pour ce fichier



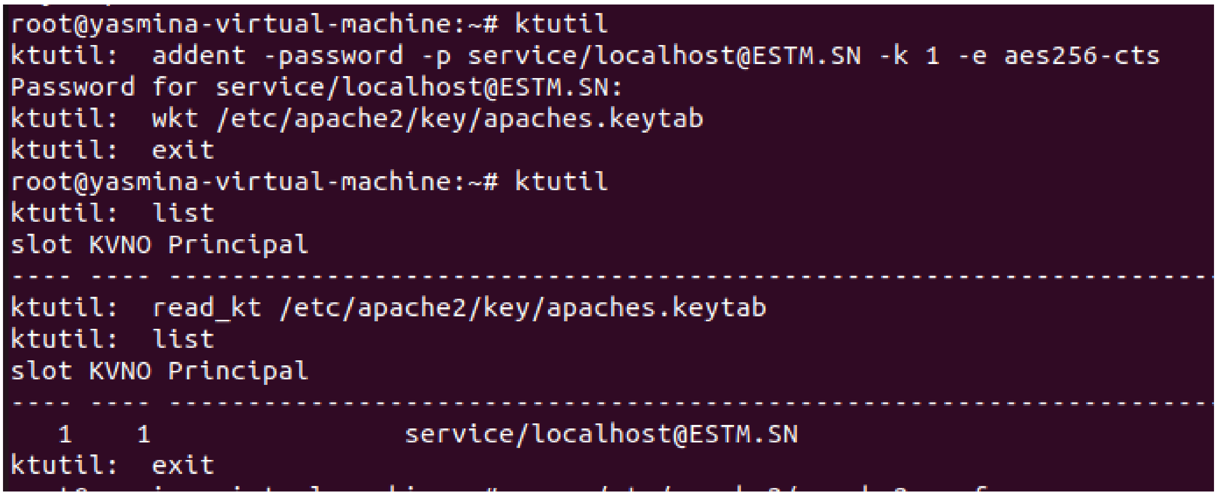
```
  GNU nano 6.2                                     /var/www/html/tp1/index.html
<!DOCTYPE html>
<html lang="fr">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Ma Page HTML</title>
</head>
<body>

    <h1>Bienvenue sur ma page HTML !</h1>

    <p>Ceci est un paragraphe de texte.</p>

    <p>Voici un lien vers <a href="https://www.example.com">Example.com</a>.</p>

    <img src="image.jpg" alt="Image">

    <form action="/submit" method="post">
        <label for="username">Nom d'utilisateur :</label><br>
        <input type="text" id="username" name="username"><br>
        <label for="password">Mot de passe :</label><br>
        <input type="password" id="password" name="password"><br><br>
        <input type="submit" value="Soumettre">
                                                  [ Read 28 lines ]
```

A l'intérieur de apache on fait ce lien entre kerberos et apache



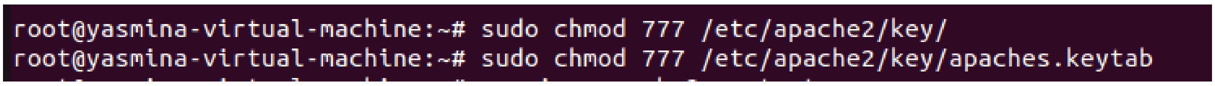
```
  GNU nano 6.2                                /etc/apache2/apache2.conf
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.


<Directory /var/www/html/tp1>
    AuthType Kerberos
    AuthName "Kerberos Authentication"
    KrbAuthRealms ESTM.SN
    KrbServiceName service/localhost@ESTM.SN
    Krb5Keytab /etc/apache2/key/apaches.keytab
    Require valid-user
</Directory>
```

Ensuite on génée cette clé dans le fichier apaches.keytab

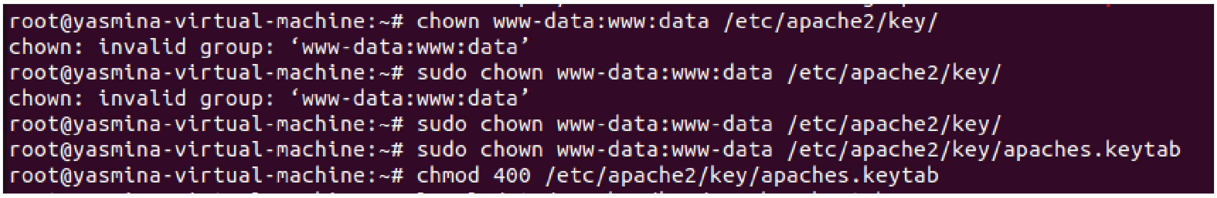


```
root@yasmina-virtual-machine:~# ktutil
ktutil:  addent -password -p service/localhost@ESTM.SN -k 1 -e aes256-cts
Password for service/localhost@ESTM.SN:
ktutil:  wkt /etc/apache2/key/apaches.keytab
ktutil:  exit
root@yasmina-virtual-machine:~# ktutil
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
ktutil:  read_kt /etc/apache2/key/apaches.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    1                 service/localhost@ESTM.SN
ktutil:  exit
```

On donne les autorisations

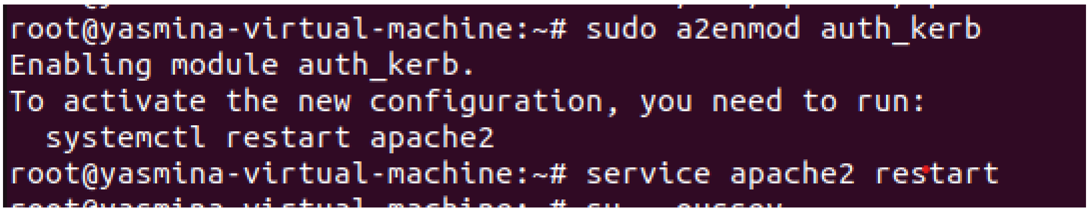


```
root@yasmina-virtual-machine:~# sudo chmod 777 /etc/apache2/key/
root@yasmina-virtual-machine:~# sudo chmod 777 /etc/apache2/key/apaches.keytab
```



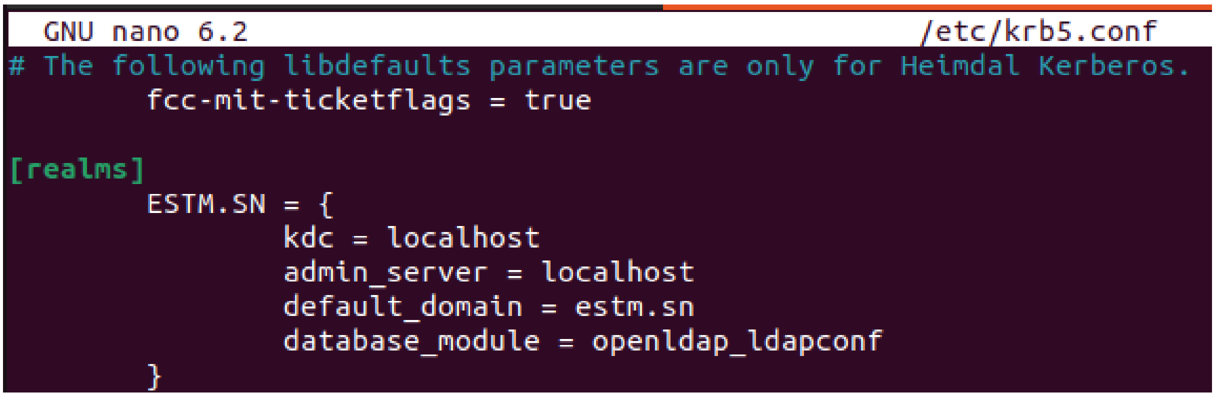
```
root@yasmina-virtual-machine:~# chown www-data:www:data /etc/apache2/key/
chown: invalid group: 'www-data:www:data'
root@yasmina-virtual-machine:~# sudo chown www-data:www:data /etc/apache2/key/
chown: invalid group: 'www-data:www:data'
root@yasmina-virtual-machine:~# sudo chown www-data:www-data /etc/apache2/key/
root@yasmina-virtual-machine:~# sudo chown www-data:www-data /etc/apache2/key/apaches.keytab
root@yasmina-virtual-machine:~# chmod 400 /etc/apache2/key/apaches.keytab
```

Après cela on active le auth_kerb



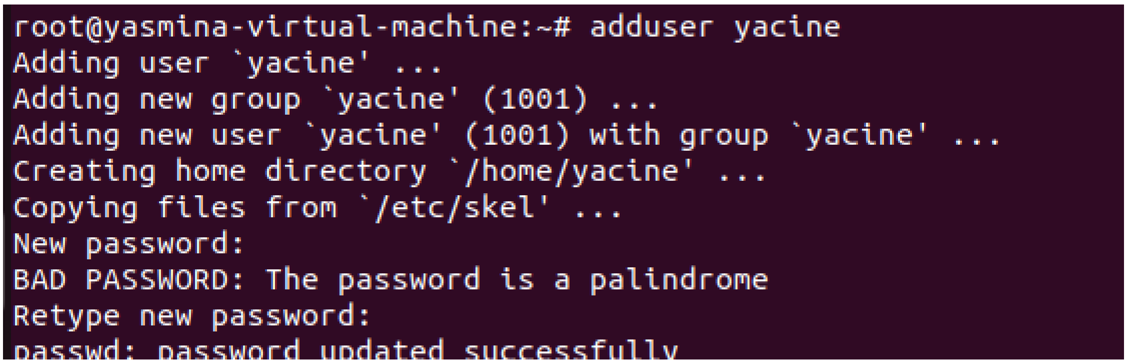
```
root@yasmina-virtual-machine:~# sudo a2enmod auth_kerb
Enabling module auth_kerb.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@yasmina-virtual-machine:~# service apache2 restart
```

Et dans le fichier krb5 on défini les paramétres de KDC



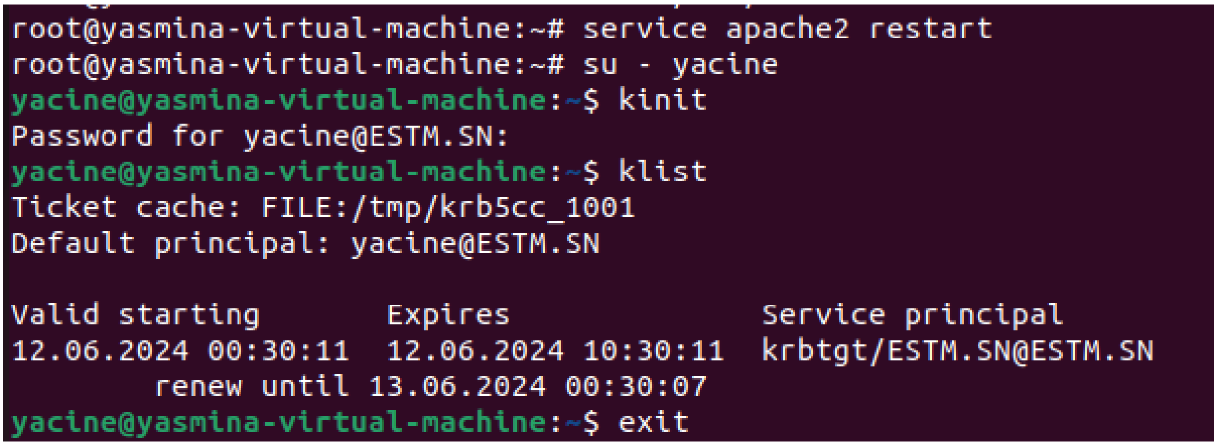
```
  GNU nano 6.2                                                 /etc/krb5.conf
# The following libdefaults parameters are only for Heimdal Kerberos.
        fcc-mit-ticketflags = true

[realms]
        ESTM.SN = {
                kdc = localhost
                admin_server = localhost
                default_domain = estm.sn
                database_module = openldap_ldapconf
        }
```

Après cela on ajoute un utilisateur



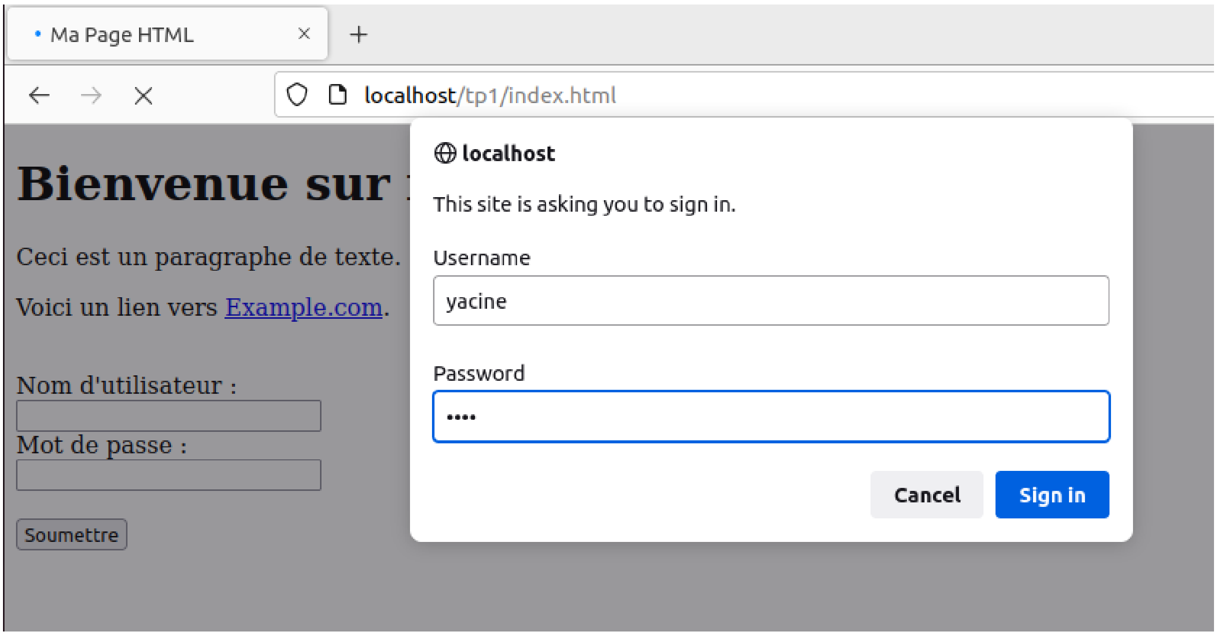
```
root@yasmina-virtual-machine:~# adduser yacine
Adding user `yacine' ...
Adding new group `yacine' (1001) ...
Adding new user `yacine' (1001) with group `yacine' ...
Creating home directory `/home/yacine' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
```

Enfin on démarre apache et demander un ticket pour l'utilisateur Yacine



```
root@yasmina-virtual-machine:~# service apache2 restart
root@yasmina-virtual-machine:~# su - yacine
yacine@yasmina-virtual-machine:~$ kinit
Password for yacine@ESTM.SN:
yacine@yasmina-virtual-machine:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: yacine@ESTM.SN

Valid starting       Expires              Service principal
12.06.2024 00:30:11  12.06.2024 10:30:11  krbtgt/ESTM.SN@ESTM.SN
        renew until 13.06.2024 00:30:07
yacine@yasmina-virtual-machine:~$ exit
```

On s’authentifie



Ma Page HTML

localhost/tp1/index.html

Bienvenue sur

Ceci est un paragraphe de texte.

Voici un lien vers Example.com.

Nom d'utilisateur :

Mot de passe :

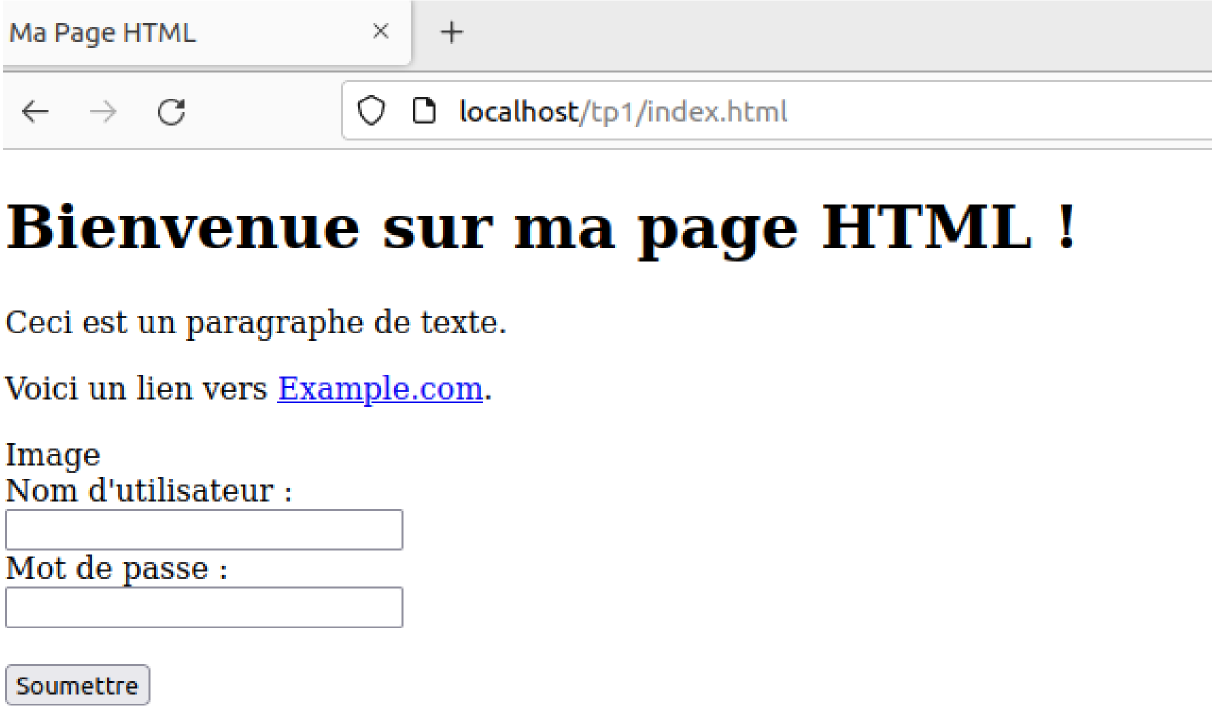
localhost

This site is asking you to sign in.

Username: yacine

Password: ••••

Et voila on peut maintenant accéder a notre site



Ma Page HTML

localhost/tp1/index.html

Bienvenue sur ma page HTML !

Ceci est un paragraphe de texte.

Voici un lien vers Example.com.

Image
Nom d'utilisateur :

Mot de passe :