TP: LDAP

Objectif

Ce TP vous permettra de mettre en place un serveur LDAP avec des données utilisateur de base. Vous pouvez ensuite explorer d'autres fonctionnalités avancées telles que la définition de schémas personnalisés, la gestion des groupes, etc., en fonction de vos besoins spécifiques.

1. **Installation d'OpenLDAP :**

Installez le serveur OpenLDAP sur votre machine Linux en utilisant la commande suivante :

```
root@tp:~# apt update
```

```
root@tp:~# apt install slapd ldap-utils
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  ldap-utils slapd
```

2. **Configuration initiale :**

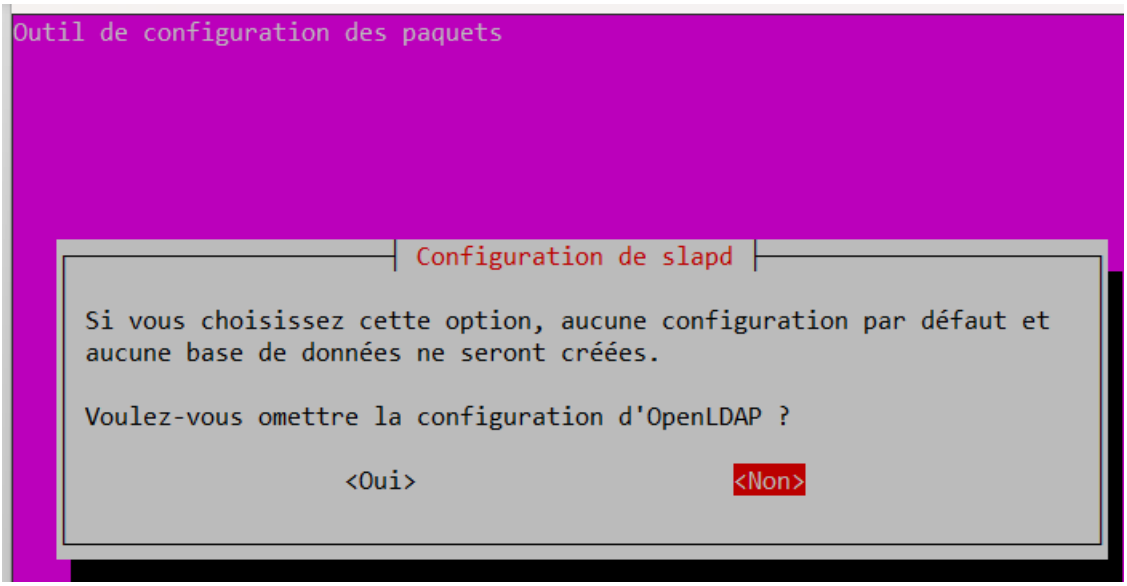
Pendant l'installation, vous serez invité à définir un mot de passe pour le compte administrateur (cn=admin,dc=smarttic,dc=sn). Notez ce mot de passe, car vous en aurez besoin pour accéder à l'annuaire LDAP en tant qu'administrateur.

3. **Configuration du serveur :**

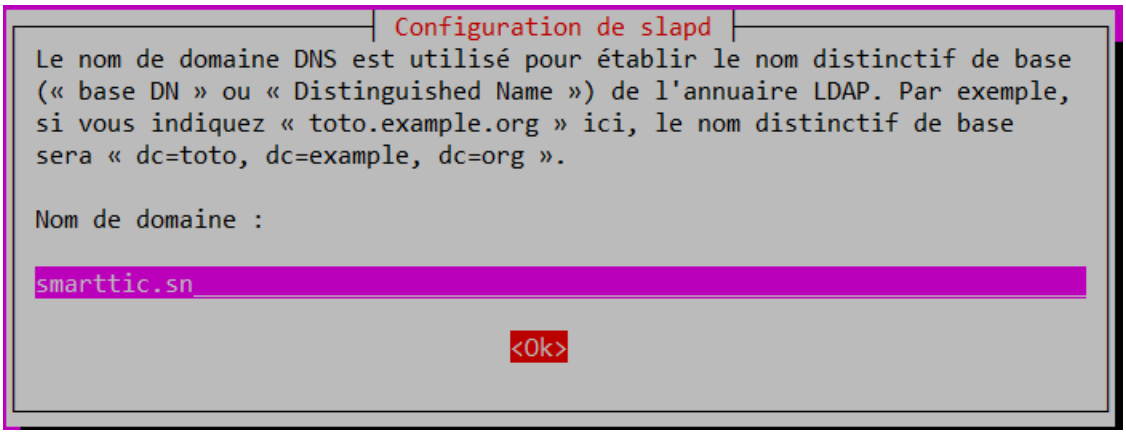
Utilisez la commande **dpkg-reconfigure slapd** pour reconfigurer le serveur LDAP.

Choisissez les options suivantes :

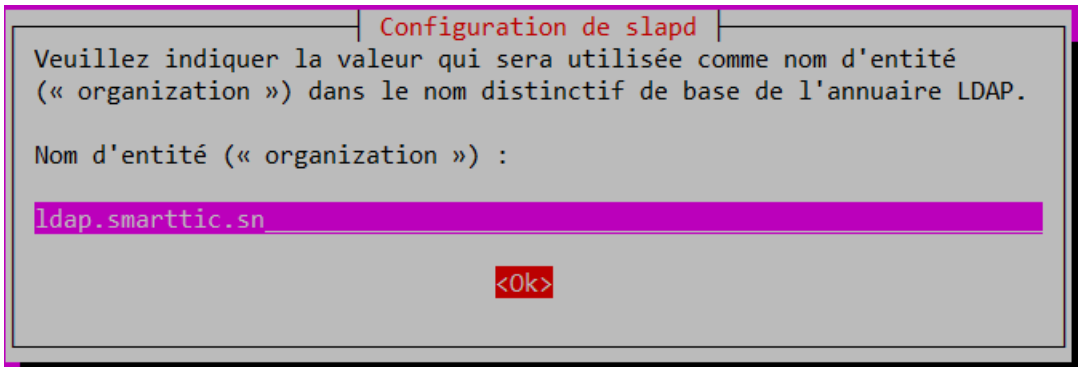
- Omettre la configuration initiale : Non



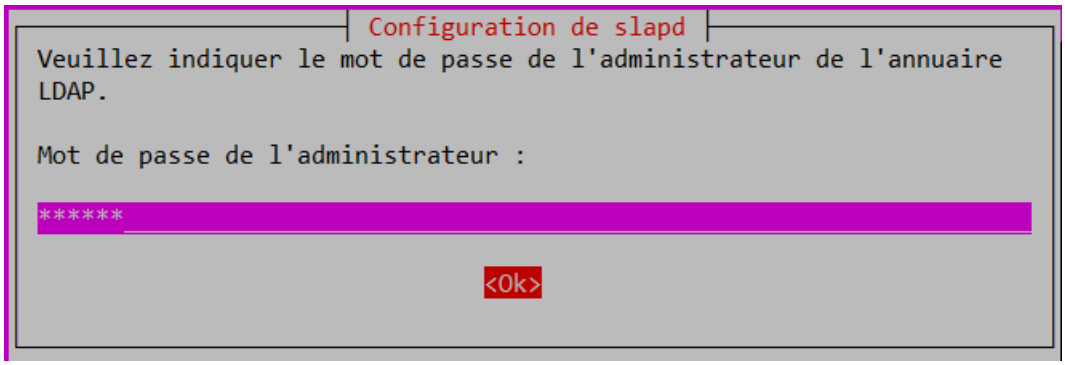
- Nom de domaine DNS : smarttic.sn



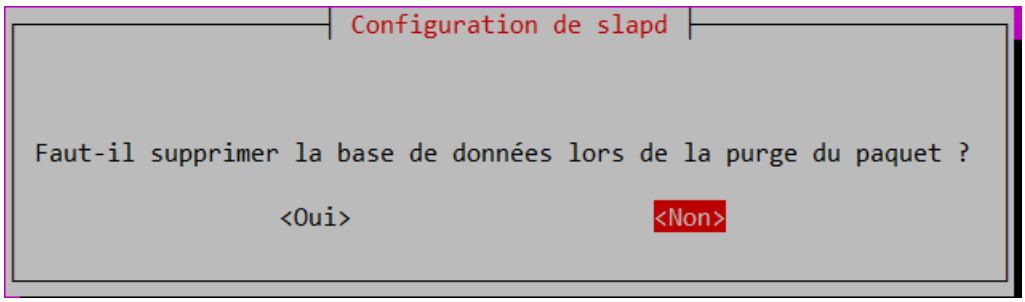
- Nom de l'organisation : ldap.smarttic.sn



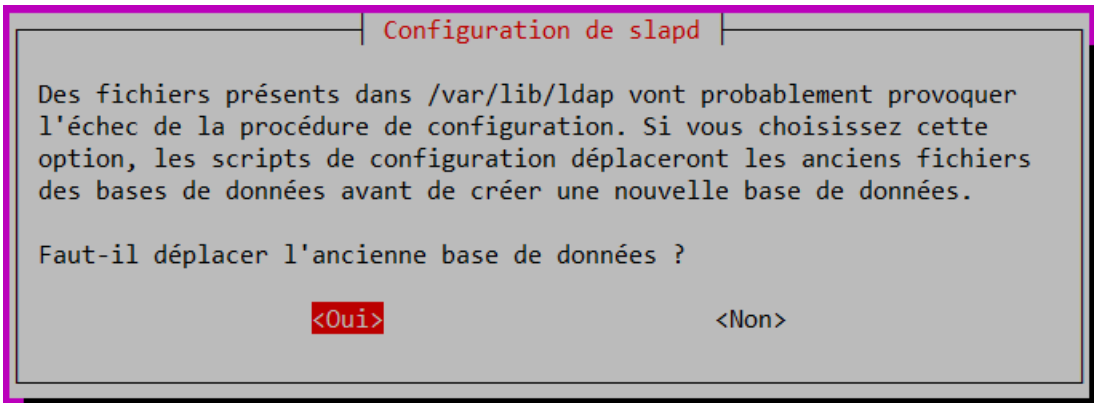
- Mot de passe administrateur : Utilisez celui que vous avez défini lors de l'installation



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



- Déplacer l'ancienne base de données :



4. **Peupler l'annuaire :**

Créez un fichier LDIF (LDAP Data Interchange Format) pour ajouter des données à l'annuaire. Voici un exemple de fichier users.ldif

```
 GNU nano 4.8                          users.ldif
dn: ou=people,dc=smarttic,dc=sn
objectClass: organizationalUnit
ou: people

dn: uid=user1,ou=people,dc=smarttic,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
cn: User One
sn: One
uid: user1
uidNumber: 2001
gidNumber: 2001
homeDirectory: /home/user1
loginShell: /bin/bash
```

5. **Ajout des données :**

Utilisez la commande suivante pour ajouter les données du fichier LDIF à l'annuaire LDAP en tant qu'administrateur :

```
root@tp:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=smarttic,dc=sn -W -f users.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=smarttic,dc=sn"

adding new entry "uid=user1,ou=people,dc=smarttic,dc=sn"

root@tp:/etc/ldap/schema#
```

Vous serez invité à saisir le mot de passe administratif que vous avez défini précédemment.

6. **Vérification des données :**

Utilisez une commande LDAP de recherche pour vérifier que les données ont été ajoutées avec succès :

```
root@tp:/etc/ldap/schema# ldapsearch -x -LLL -b dc=smarttic,dc=sn "(objectClass=inetOrgPerson)"
dn: uid=user1,ou=people,dc=smarttic,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
cn: User One
sn: One
uid: user1
uidNumber: 2001
gidNumber: 2001
homeDirectory: /home/user1
loginShell: /bin/bash
```

7. **Nettoyage (facultatif) :**

Si vous souhaitez supprimer les données que vous avez ajoutées, utilisez la commande ldapdelete avec les DN appropriés.

TP2 : Création de groupe dans l'annuaire LDAP

Ce TP vous guidera à travers la création de deux groupes "it" et "rhs" dans votre annuaire LDAP. Vous pouvez ensuite ajouter des membres aux groupes et explorer d'autres fonctionnalités de gestion des groupes selon vos besoins spécifiques.

Étapes du TP pour créer deux groupes LDAP :

Par conséquent, nous allons créer le fichier de groupes de base comme suit.

1. **Configurer le groupe de base pour les utilisateurs OpenLDAP**

L'étape suivante consiste à créer un nouveau groupe de base pour les utilisateurs OpenLDAP. Pour démontrer cela, nous allons créer deux groupes de base : les personnes et les groupes . Le groupe « personnes » sera utilisé pour stocker les utilisateurs réguliers tandis que le groupe « groupes » stockera les groupes sur votre serveur LDAP.

```
 GNU nano 4.8                                    base-groups.ldif
dn: ou=peoples,dc=smarttic,dc=sn
objectClass: organizationalUnit
ou: peoples

dn: ou=groupes,dc=smarttic,dc=sn
objectClass: organizationalUnit
ou: groupes
```

Pour ajouter les groupes de base, exécutez la commande ' ldapadd ' sur le fichier 'base-groups.ldif'. Fournissez le mot de passe administrateur OpenLDAP lorsque vous y êtes invité et appuyez sur « ENTRÉE ».

```
root@tp:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=smarttic,dc=sn -W -f base-groups.ldif
Enter LDAP Password:
adding new entry "ou=peoples,dc=smarttic,dc=sn"

adding new entry "ou=groupes,dc=smarttic,dc=sn"

root@tp:/etc/ldap/schema#
```

2. **Ajouter un nouveau groupe au groupe de base :**

Avec les groupes de base déjà créés, dans cette section, nous allons procéder à l'ajout d'un nouveau groupe au groupe de base « groupes ».

Créez un fichier LDIF nommé group.ldif avec les définitions des groupes "support_it" et "support_rhs" :

```
  GNU nano 4.8                                          group.ldif
dn: cn=support_it,ou=groupes,dc=smarttic,dc=sn
objectClass: posixGroup
cn: support_it
gidNumber: 5000

dn: cn=support_rhs,ou=groupes,dc=smarttic,dc=sn
objectClass: posixGroup
cn: support_rhs
gidNumber: 6000
```

3. **Ajout des groupes à l'annuaire LDAP :**

Utilisez la commande suivante pour ajouter les groupes du fichier LDIF à l'annuaire LDAP en tant qu'administrateur :

```
root@tp:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=smarttic,dc=sn -W -f group.ldif
Enter LDAP Password:
adding new entry "cn=support_it,ou=groupes,dc=smarttic,dc=sn"

adding new entry "cn=support_rhs,ou=groupes,dc=smarttic,dc=sn"

root@tp:/etc/ldap/schema#
```

4. **Vérification des groupes :**

Utilisez la commande LDAP de recherche pour vérifier que les groupes ont été ajoutés avec succès :

```
root@tp:/etc/ldap/schema# ldapsearch -x -LLL -b dc=smarttic,dc=sn '(cn=support_it)' gidNumber
dn: cn=support_it,ou=groups,dc=smarttic,dc=sn
gidNumber: 5000

dn: cn=support_it,ou=groupes,dc=smarttic,dc=sn
gidNumber: 5000

root@tp:/etc/ldap/schema# ldapsearch -x -LLL -b dc=smarttic,dc=sn '(cn=support_rhs)' gidNumber
dn: cn=support_rhs,ou=groups,dc=smarttic,dc=sn
gidNumber: 6000

dn: cn=support_rhs,ou=groupes,dc=smarttic,dc=sn
gidNumber: 6000

root@tp:/etc/ldap/schema#
```

5. Créez un nouvel utilisateur OpenLDAP

La dernière étape consiste à créer un utilisateur OpenLDAP et à attacher l'utilisateur à un groupe de base spécifique.

Ensuite, créez un nouveau fichier utilisateur comme indiqué.

```
 GNU nano 4.8                                    user.ldif
dn: uid=bousso,ou=peoples,dc=smarttic,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: bousso
sn: mame
givenName: bousso
cn: bousso mame
displayName: bousso mame
uidNumber: 7000
gidNumber: 7000
userPassword: passer123
gecos: Bousso Mame
loginShell: /bin/bash
homeDirectory: /home/bousso
```

Dans cette configuration, nous créons un nouvel utilisateur appelé « bousso » avec un UID de 7 000. Le répertoire personnel par défaut sera « /home/bousso » et le shell de connexion par défaut « /bin/bash ». Le nouvel utilisateur fera partie du groupe de base appelé « personnes » avec un GID de 7 000.

```
root@tp:/etc/ldap/schema# ldapadd -x -D cn=admin,dc=smarttic,dc=sn -W -f user.ldif
Enter LDAP Password:
adding new entry "uid=bousso,ou=people,dc=smarttic,dc=sn"

root@tp:/etc/ldap/schema#
```

```
root@tp:/etc/ldap/schema# ldapsearch -x -LLL -b dc=smarttic,dc=sn '(uid=bousso)' cn uidNumber gidNumber
dn: uid=bousso,ou=people,dc=smarttic,dc=sn
cn: alex mame
uidNumber: 7000
gidNumber: 7000

root@tp:/etc/ldap/schema#
```