2012

Dossier LDAP-STESIO

Classe de BTS SIO 1

Lycée Blaise Pascal

23/05/2012

Sommaire

Introduction

Ce dossier est une synthèse des démarches effectuées au cours du 2ème semestre de l'année scolaire 2011 – 2012 pour la mise en place d'un serveur d'authentification.

Notre entreprise nommée STESIO à été créée au sein de la section BTS SIO (Système Informatique aux Organisations).

Cette entreprise à pour but de délivrer des services qui s'appuient sur des nouvelles et qui permettent aux administrateurs et aux entreprises d'être plus efficaces. Grâce à notre expertise, des technologies de l'information, nous sommes en mesure de prendre en charge l'externalisation des processus métier de nos entreprises clientes. Nous permettons donc à nos clients de se recentrer sur leur métier.

Pour ce projet, nous avons dû mettre en place un annuaire permettant de répertorier les machines et sessions GNU/Linux de notre réseau, un serveur d'authentification permettant de se connecter à nos sessions réseau et un serveur NFS dont le but est de centraliser les dossiers personnels des utilisateurs du réseau. Ce serveur utilise la technologie RAID 1, afin d'améliorer la tolérance de panne.

Présentation du Projet

I/ Les Besoins :

Nous avions besoin de recenser les machines et les sessions utilisateurs, grâce à un serveur GNU/Linux sécurisé tout en offrant une tolérance de panne convenable.

II/ Les Objectifs :

Nous devions respecter notre cahier des charges par rapport aux différentes contraintes citées ci-après. Pour répondre à notre cahier des charges, nous avons donc mis en place un serveur LDAP-PAM-NFS.

III/ Le Cahier des Charges :

Notre professeur a élu deux chefs de projet pour mener à bien ce projet : **ROUSSEAU Clément** et **OUACHAIN Benoît**, qui devaient s'assurer de la continuité du projet. Nous avons ensuite réparti les groupes en fonction des modules à étudier.

Notre professeur nous a fourni un PC que nous avons donc transformé en serveur. Nous devions mettre en place les modules LDAP, PAM et NFS. Nous devions implémenter la technologie RAID 1, et disposant d'un PC classique comme serveur, nous avons donc implémenté du RAID 1 logiciel.

IV/ Les Contraintes :

Nous devions d'abord comprendre le fonctionnement et l'objectif de chaque module avant de pouvoir essayer de les mettre en place. Nous avons ensuite compris que les modules étaient dépendant les uns des autres, et que par exemple on ne pouvait pas essayer de faire fonctionner PAM sans avoir au préalable mis en place LDAP. Nos groupes répartis suivant les modules ne servaient donc plus à rien.

V/ Choix de la solution :

Nous avons choisi d'utiliser la distribution Debian pour notre serveur, celle-ci étant la distribution pour serveur la mieux maîtrisée par nous tous et la plus adaptée étant donné sa stabilité. Afin de gérer notre arborescence LDAP, nous avons choisi d'utiliser l'interface web LAM (LDAP Account Manager), qui est simple d'utilisation et qui rend notre serveur LDAP administrable de n'importe où.

Suivi du Projet

I/ Diagramme de Gantt Prévisionnel :

Cf. annexe.

II/ Diagramme de Gantt réel :

Cf. annexe.

III/ Les problèmes rencontrés :

Au fil de notre projet, nous avons évidement rencontré des problèmes.
Dans un premier temps, nous devions comprendre le fonctionnement de chacun des modules avant de nous atteler à leur installation.
Les fiches de procédures que nous avons trouvées sur internet correspondaient à des anciennes versions des modules, les fichiers de configurations n'étaient pas les mêmes, ce qui nous a fait perdre du temps.
Par la suite, nous nous sommes rendu compte que les modules étaient dépendant les uns des autres. Nous avons donc modifié la disposition des groupes.
Un autre problème a été rencontré, celui de l'interconnexion entre PAM et LDAP. Il s'agissait en faite d'une erreur dans la commande :
Le client pointait sur l'adresse ldapi://IP_DU_SERVEUR au lieu de ldap://IP_DU_SERVEUR.

Mise en place de la solution

I/ Explications, commandes, mise en place… :

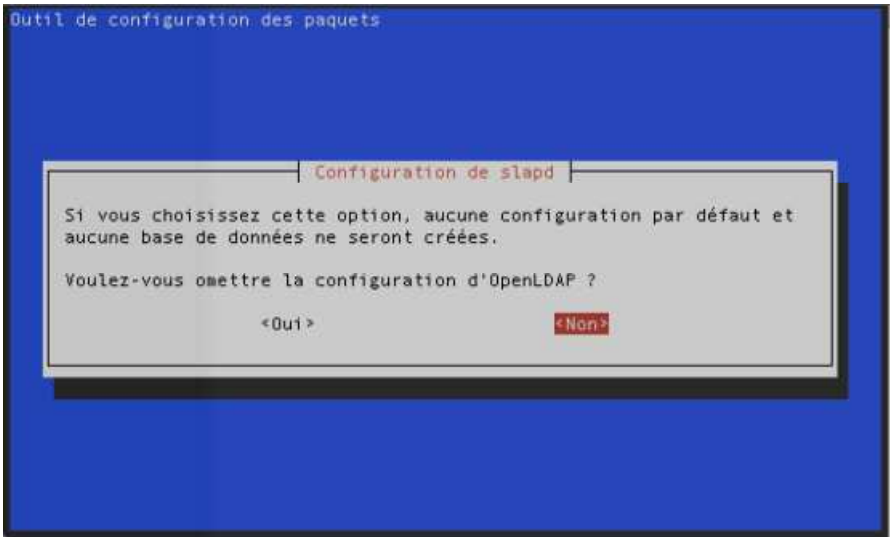
Tout d'abord, il faut installer le RAID 1 lors de l'installation de Debian.

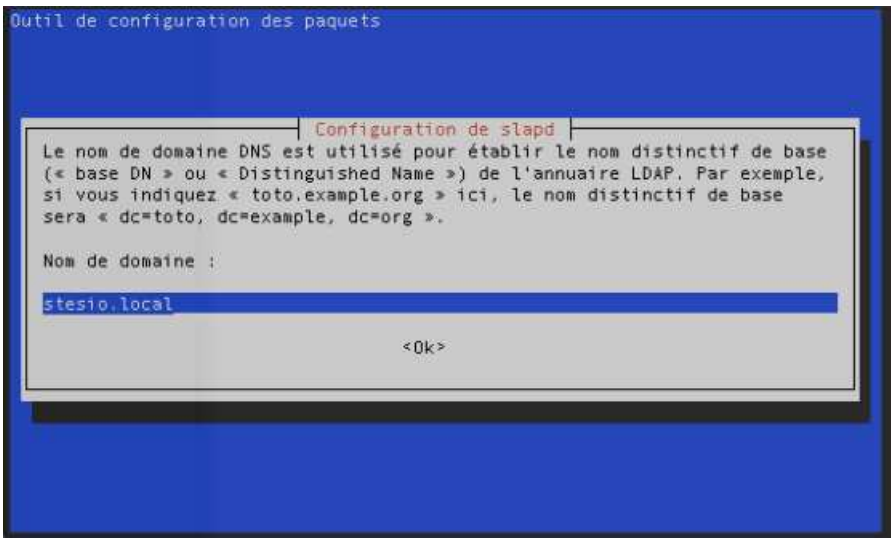
1. Fiche de procédure pour RAID 1 :

Cf. annexe

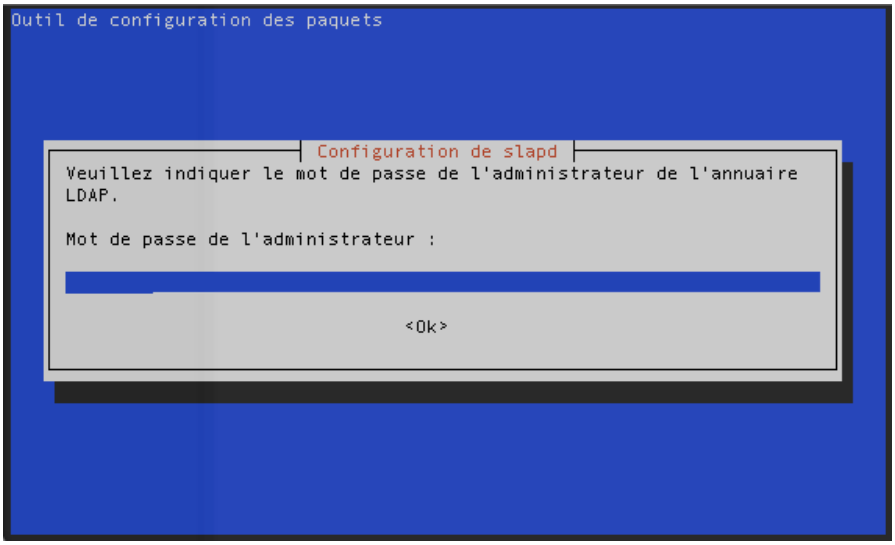
2. Installation d'OpenLDAP :

Premièrement, nous devons installer OpenLDAP.
Il faut installer les paquets ldap-client slapd ldap-utils
On effectue ensuite un dpkg-reconfigure slapd
Suivez ensuite les captures d'écran :






Outil de configuration des paquets
Configuration de slapd
Veuillez indiquer la valeur que sera utilisée comme nom d'entité
(« organization ») dans le nom distinctif de base de l'annuaire LDAP.
Nom d'entité (« organization ») :
stesio.local
<Ok>


Outil de configuration des paquets
Configuration de slapd
Veuillez indiquer le mot de passe de l'administrateur de l'annuaire
LDAP.
Mot de passe de l'administrateur :
<Ok>


Outil de configuration des paquets
Configuration de slapd
Le module HDB est recommandé. HDB et BDB utilisent des formats de
stockage analogues. Par contre, HDB gère les renommages de sous-arbres.
Les deux formats utilisent les mêmes options de configuration.
Quel que soit votre choix, vous devriez adapter les options de
configuration à vos besoins. Pour plus d'informations, veuillez
consulter le fichier /usr/share/doc/slapd/README.DB_CONFIG.gz.
Module de base de données à utiliser :
BDB
HDB
<Ok>

On n’active pas le protocole LDAPv2. Nous en sommes à la version 3.
Notre nom d’administrateur est cn=admin,dc=stesio,dc=local.
Notre mot de passe est celui que nous avons indiqué plus tôt dans l’installation d’OpenLDAP.

3. Les fichiers LDIF et leur syntaxe :

L'ajout d'objets dans l'annuaire peut s'effectuer de plusieurs manières.
On peut utiliser le client LDAPadmin pour Windows, ou l'interface web LAM (LDAP Account Manager).
L'utilisation de LAM sera expliquée un peu plus loin.
Il est aussi possible de créer des fichiers LDIF contenant les différents objets, tels que les utilisateurs, les groupes, etc… Les fichiers LDIF ont une syntaxe particulière, exemple :

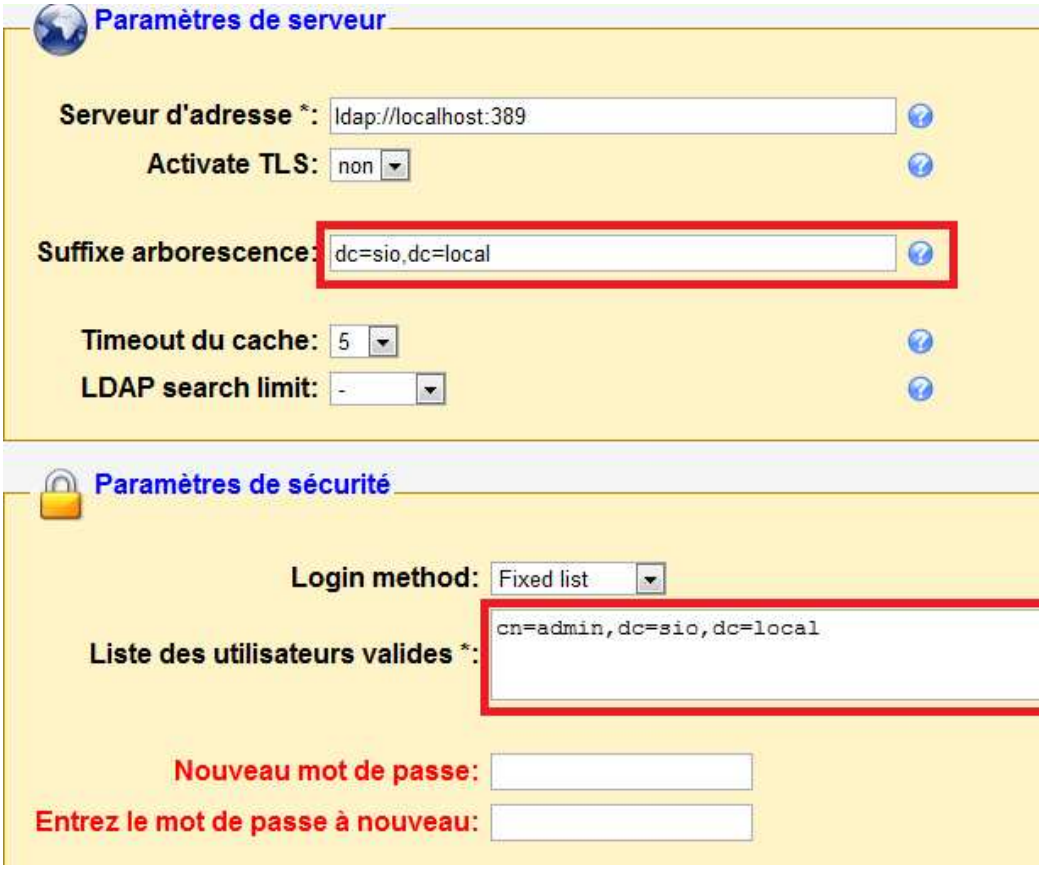
```
version: 1

# Export LDIF pour: ou=People,dc=sio,dc=local
# Scope de recherche: base
# Filtre de recherche: (objectClass=*)
# Entrées total: 1

# Entrée 1: ou=People,dc=sio,dc=local
dn: ou=People,dc=sio,dc=local
objectClass: organizationalUnit
ou: People
```

Enregistrez votre fichier .LDIF où vous voulez, le mieux est de créer un répertoire pour les rassembler.
Une fois votre fichier créé, il faut l'importer dans l'annuaire.
Voici la commande pour le faire :
ldapadd –x –D "cn=admin,dc=stesio,dc=local" –W –f NotreFichier.ldif

4. Installation et fonctionnement de LDAP Account Manager

Afin de gérer notre annuaire grâce à une interface, installer les paquets suivants :
apache2 php5 ldap-account-manager
Configuration de LAM avec la commande dpkg-reconfigure ldap-account-manager
Une fois installé, il faut ouvrir un navigateur et saisir http://IP_DU_SERVEUR/lam afin d'accéder à l'interface web.
Vous remarquerez que l'utilisateur proposé par défaut sous LAM est Manager, alors que notre utilisateur est nommé admin (cn=admin,dc=stesio,dc=local).
Cliquez en haut à gauche sur Configuration de LAM, puis sur Editer les paramètres globaux. Le mot de passe par défaut est lam.
En bas de la page, vous pouvez choisir le nouveau mot de passe de

configuration de LAM. Cliquez ensuite sur OK.
Cliquez de nouveau sur Configuration de LAM, puis sur Editer les profils. Tapez le mot de passe des profils, qui par défaut est aussi lam.



Dans Suffixe arborescence indiquez notre nom de domaine.
Dans liste des utilisateurs valides, tapez notre nom d'utilisateur (cn=admin,dc=stesio,dc=local), ce qui remplacera Manager par admin.
Choisissez ensuite un nouveau mot de passe, puis cliquez sur le bouton Sauvegarder en haut à droite de la page.
Vous pouvez enfin vous connecter pour gérer les utilisateurs, groupes et machines du réseau.

5. Activer les logs pour OpenLDAP

Afin d'activer les logs d'OpenLDAP, nous devons modifier le fichier de configuration de LDAP et y ajouter le niveau de log 256.

Modifiez le fichier /etc/ldap/slapd.d/ /olcDatabase={0}config.ldif
Et y ajouter la ligne suivante :
olcLogLevel : 256
Modifiez ensuite le fichier /etc/rsyslog.conf
Et ajoutez-y :
Local4.* /var/log/ldap.log

6. Installation du serveur NFS

Afin d'installer le serveur NFS, il faut installer les paquets suivants :
nfs-kernel-server nfs-common portmap
Il nous faut ensuite modifier le fichier /etc/exports et y ajouter la ligne :
/home 192.168.1.0/24(rw,sync,no_subtree_check,root_squash)
Cette ligne sert à déporter le /home du serveur vers tout les clients NFS du réseau 192.168.1.0 et donne les droits d'écriture-lecture, et de réduction des droits pour un utilisateur root.
Redémarrez le serveur NFS : /etc/init.d/nfs-kernel-server restart

7. Authentification OpenLDAP sur les clients

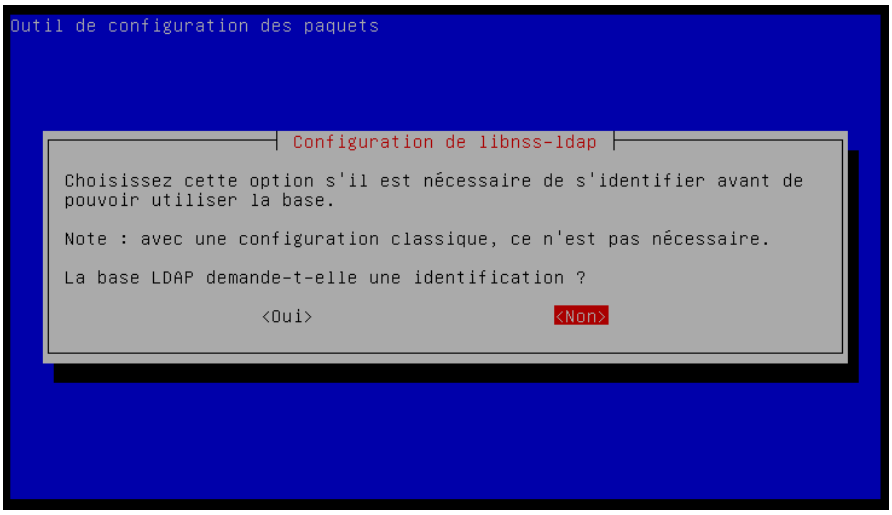
Attention ! Les commandes indiquées ici sont pour un client sous Debian. Sur Ubuntu par exemple, les commandes seront pratiquement les mêmes, mais il faudra activer l'authentification LDAP pour GDM ou KDM dans les fichiers de configuration de PAM.
Sous Ubuntu 11, le gestionnaire de connexion n'est plus GDM mais LightDM, et nous n'avons donc pas réussi à activer l'authentification LDAP pour ce service.

Afin d'activer l'authentification LDAP sur les clients, il faut installer les paquets suivants :
nscd libnss-ldap libpam-ldap
Tapez ensuite la commande dpkg-reconfigure libnss-ldap, puis suivez les copies d'écran ci-dessous :
Attention ! Faites bien en sorte d'effacer la lettre 'i' dans ldap**i**://ID_DU_SERVEUR/
Sinon, cela ne fonctionnera pas !

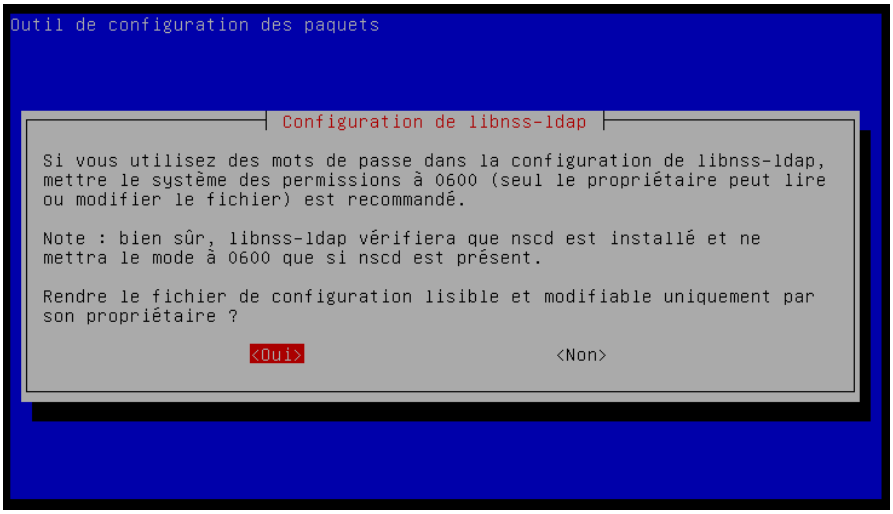

Outil de configuration des paquets
Configuration de libnss-ldap
Veuillez indiquer l'URI d'accès au serveur LDAP. Il s'agit en général d'une chaîne de caractères sous la forme « ldap://<hôte ou IP>:<port>/ ». Des URI utilisant « ldaps:// » ou « ldapi:// » sont également possibles. Le numéro de port est facultatif.
Note : utiliser une adresse IP est recommandé ; les risques d'échec sont réduits en cas d'indisponibilité du service de noms.
URI du serveur LDAP :
ldap://192.168.1.10/
<Ok>

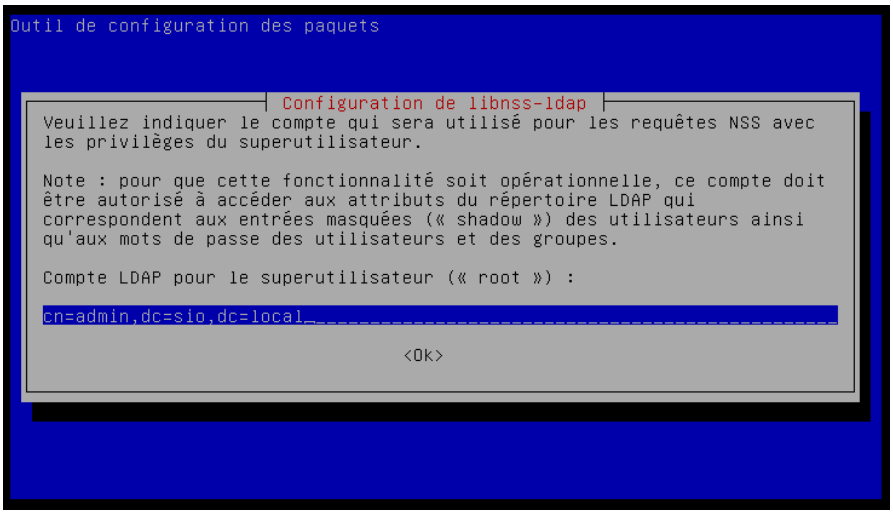

Outil de configuration des paquets
Configuration de libnss-ldap
Veuillez indiquer le nom distinctif de la base de recherche. Beaucoup de sites utilisent ici les composants de leurs noms de domaine. Ainsi, pour le domaine « exemple.net », le nom distinctif utilisé serait « dc=exemple,dc=net ».
Nom distinctif (DN) de la base de recherche :
dc=sio,dc=local
<Ok>


Outil de configuration des paquets
Configuration de libnss-ldap
Veuillez indiquer la version du protocole LDAP que doit utiliser ldapns. Il est recommandé de choisir le numéro de version le plus élevé disponible.
Version de LDAP à utiliser :
3
2
<Ok>

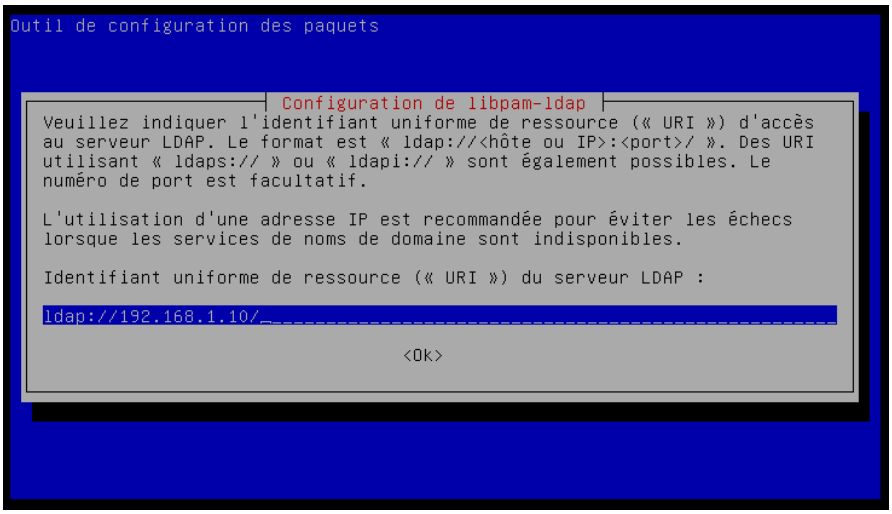

Outil de configuration des paquets
Configuration de libnss-ldap
Choisissez cette option s'il est nécessaire de s'identifier avant de pouvoir utiliser la base.
Note : avec une configuration classique, ce n'est pas nécessaire.
La base LDAP demande-t-elle une identification ?
<Oui>
<Non>


Outil de configuration des paquets
Configuration de libnss-ldap
Cette option permet aux outils qui interrogent le système NSS avec libnss-ldap de récupérer des informations supplémentaires lorsqu'ils sont utilisés par le superutilisateur (« root »).
Si vous utilisez un répertoire /etc monté par NFS ou toute autre combinaison de réglages similaire, vous devriez désactiver cette option.
Privilèges LDAP spécifiques pour le superutilisateur ?
<Oui>
<Non>

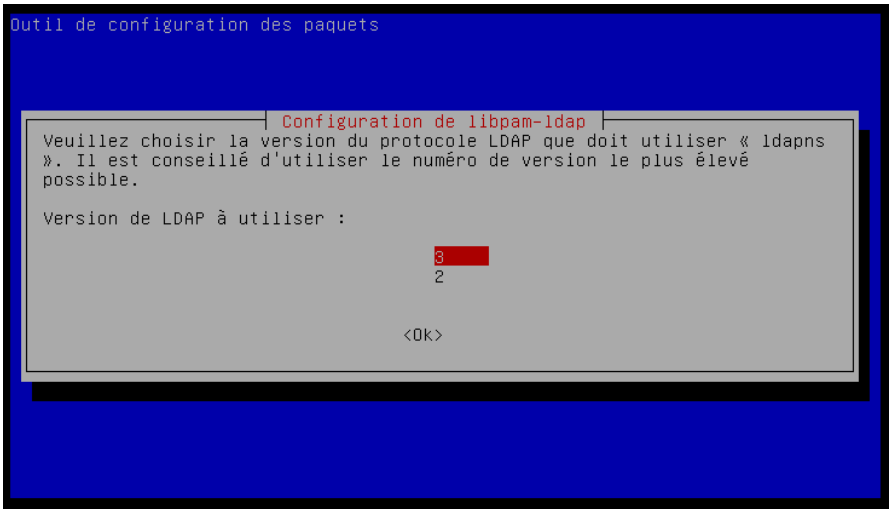

Outil de configuration des paquets
Configuration de libnss-ldap
Si vous utilisez des mots de passe dans la configuration de libnss-ldap, mettre le système des permissions à 0600 (seul le propriétaire peut lire ou modifier le fichier) est recommandé.
Note : bien sûr, libnss-ldap vérifiera que nscd est installé et ne mettra le mode à 0600 que si nscd est présent.
Rendre le fichier de configuration lisible et modifiable uniquement par son propriétaire ?
<Oui>
<Non>



Tapez ensuite la commande dpkg-reconfigure libpam-ldap.
Attention ! Faites bien en sorte d'effacer la lettre 'i' dans ldap**i**://ID_DU_SERVEUR/
Sinon, cela ne fonctionnera pas !

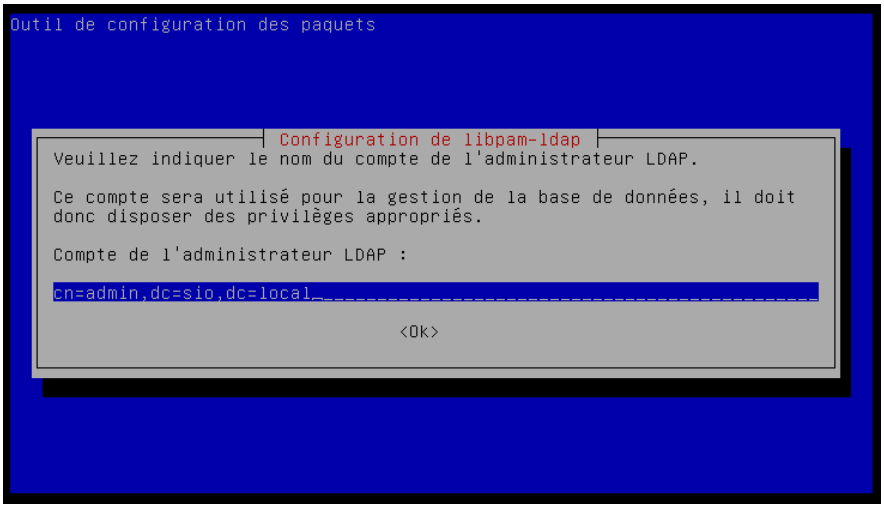

Outil de configuration des paquets
Configuration de libpam-ldap
Veuillez indiquer l'identifiant uniforme de ressource (« URI ») d'accès au serveur LDAP. Le format est « ldap://<hôte ou IP>:<port>/ ». Des URI utilisant « ldaps:// » ou « ldapi:// » sont également possibles. Le numéro de port est facultatif.
L'utilisation d'une adresse IP est recommandée pour éviter les échecs lorsque les services de noms de domaine sont indisponibles.
Identifiant uniforme de ressource (« URI ») du serveur LDAP :
ldap://192.168.1.10/
<Ok>

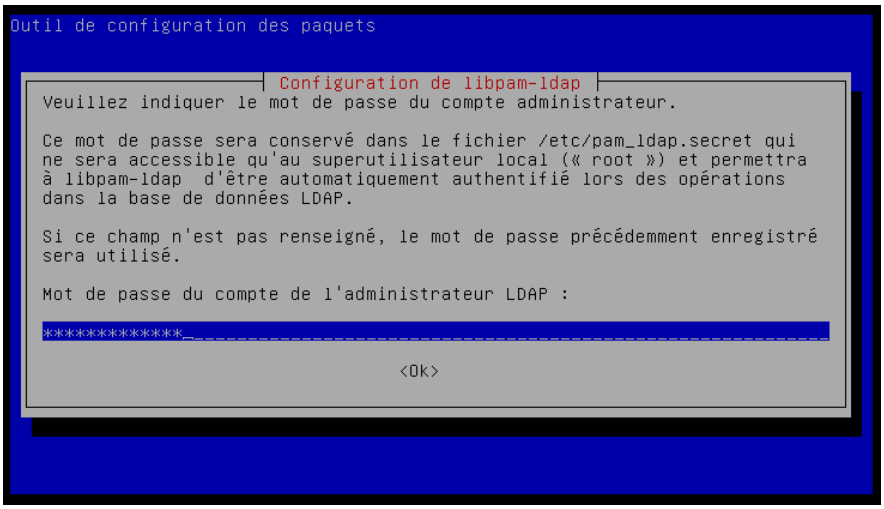

Outil de configuration des paquets
Configuration de libpam-ldap
Veuillez indiquer le nom distinctif de la base de recherche LDAP. La majorité des sites utilisent les composants de leur nom de domaine. Ainsi, pour le domaine « exemple.net », le nom distinctif utilisé serait « dc=exemple,dc=net ».
Nom distinctif (DN) de la base de recherche :
dc=sio,dc=local
<Ok>


Outil de configuration des paquets
Configuration de libpam-ldap
Veuillez choisir la version du protocole LDAP que doit utiliser « ldapns ». Il est conseillé d'utiliser le numéro de version le plus élevé possible.
Version de LDAP à utiliser :
3
2
<Ok>

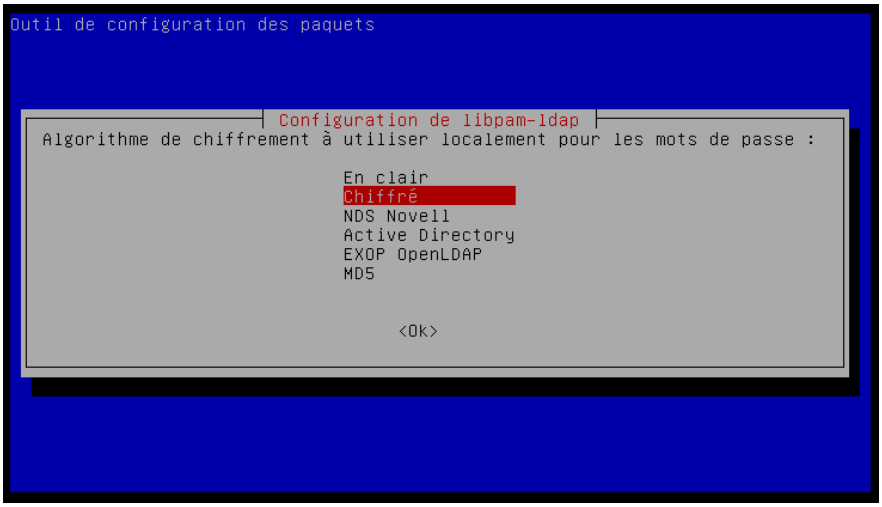

Outil de configuration des paquets
Configuration de libpam-ldap
Si vous choisissez cette option, les outils de gestion de mots de passe qui utilisent PAM pourront changer les mots de passe locaux.
Le mot de passe du compte d'administrateur LDAP sera conservé dans un fichier séparé accessible au seul superutilisateur local (« root »).
Si /etc est monté par NFS, cette option doit être désactivée.
Donner les privilèges de superutilisateur local au compte administrateur LDAP ?
<Oui>
<Non>

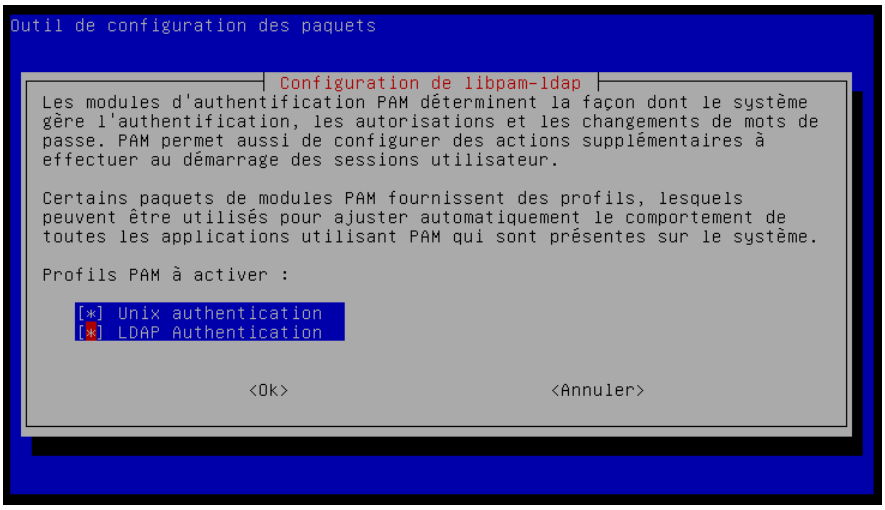

Outil de configuration des paquets
Configuration de libpam-ldap
Veuillez indiquer si le serveur LDAP nécessite une authentification pour la lecture de ses données.
Une telle configuration n'est généralement pas utile.
La base de données LDAP demande-t-elle une identification ?
<Oui>
<Non>


Outil de configuration des paquets
Configuration de libpam-ldap
Veuillez indiquer le nom du compte de l'administrateur LDAP.
Ce compte sera utilisé pour la gestion de la base de données, il doit donc disposer des privilèges appropriés.
Compte de l'administrateur LDAP :
cn=admin,dc=sio,dc=local
<Ok>


Outil de configuration des paquets
Configuration de libpam-ldap
Veuillez indiquer le mot de passe du compte administrateur.
Ce mot de passe sera conservé dans le fichier /etc/pam_ldap.secret qui ne sera accessible qu'au superutilisateur local (« root ») et permettra à libpam-ldap d'être automatiquement authentifié lors des opérations dans la base de données LDAP.
Si ce champ n'est pas renseigné, le mot de passe précédemment enregistré sera utilisé.
Mot de passe du compte de l'administrateur LDAP :
****
<Ok>


Outil de configuration des paquets
Configuration de libpam-ldap
Le module PAM peut chiffrer localement le mot de passe lors d'un changement, ce qui est le comportement recommandé :
- En clair : pas de chiffrement. Peut être choisi lorsque les serveurs LDAP chiffrent automatiquement l'attribut « userPassword »;
- Chiffré : l'attribut « userPassword » utilise le même format que les mots de passe locaux. Option à choisir en cas de doute;
- NDS : méthode « Novell Directory Services » : l'ancien mot de passe est d'abord supprimé, puis mis à jour;
- Active Directory : méthode « Active Directory » : crée un mot de passe Unicode et met à jour l'attribut « unicodePwd »;
- EXOP : méthode de changement de mot de passe d'OpenLDAP.
<Ok>


Outil de configuration des paquets
Configuration de libpam-ldap
Algorithme de chiffrement à utiliser localement pour les mots de passe :
En clair
Chiffré
NDS Novell
Active Directory
EXOP OpenLDAP
MD5
<Ok>



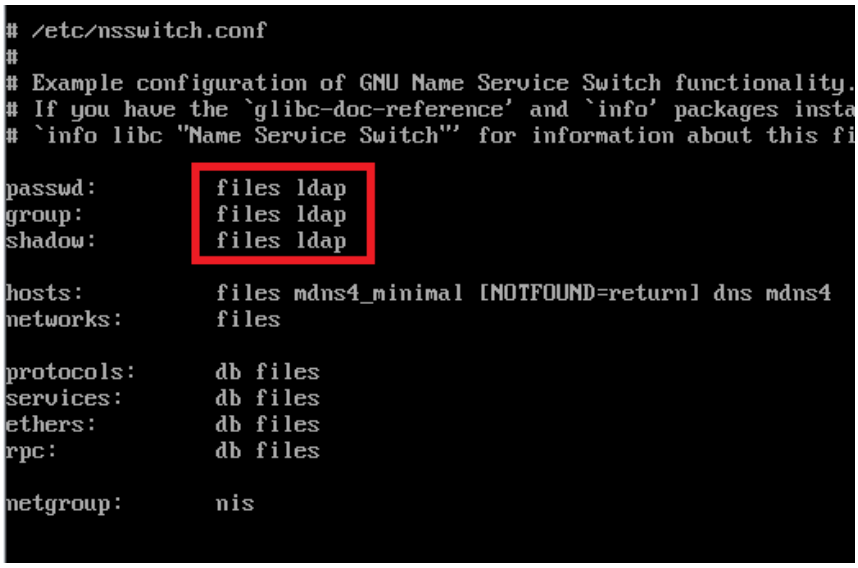
Sous Ubuntu, vous aurez peut-être besoin d'exécuter la commande dpkg-reconfigure ldap-auth-config

Une fois l'installation terminée, il faut modifier des paramètres dans le fichier /etc/nsswitch.conf pour que l'authentification LDAP fonctionne.

Sous Debian :

```
root@maxdata-315-10:~# cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Su
# If you have the `glibc-doc-reference' and `
# `info libc "Name Service Switch"' for inform

passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
```

Sous Ubuntu :



8. Mise en place du client NFS

Les commandes suivantes seront sensiblement les mêmes que ce soit pour Debian ou pour Ubuntu.
Installez les paquets nfs-client nfs-common
Ajoutez ensuite la ligne suivante dans le fichier /etc/fstab
IP_DU_SERVEUR:/home /home nfs hard,intr,rw 0 0
Redémarrez votre machine, et le dossier /home est enfin déporté sur notre serveur.

Conclusion

Ce projet nous a permis de nous habituer à un travail de groupe, de nous donner une approche d'un projet professionnel, mais aussi d'acquérir de nouvelles connaissances.