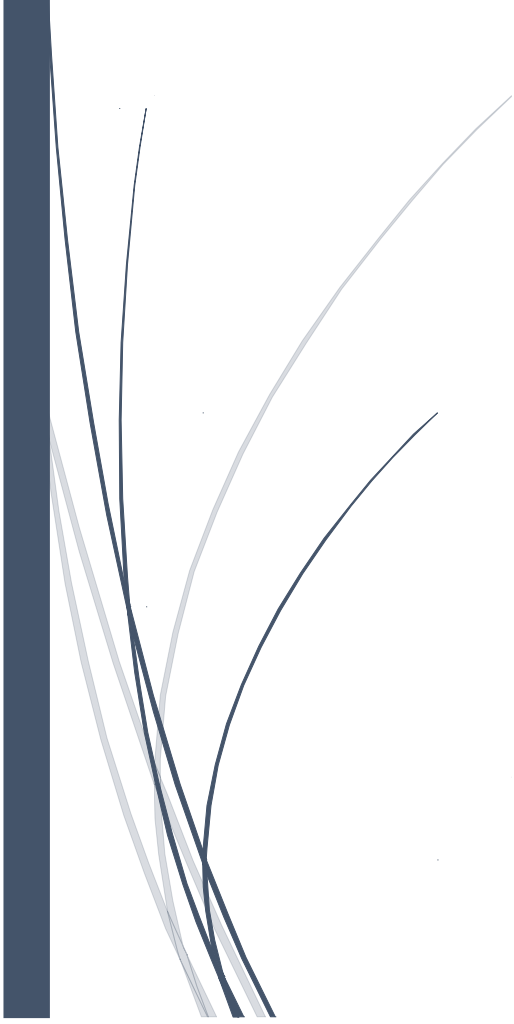
08/01/2015

Installation d'un serveur SAMBA/LDAP

V1



Lecaudey Etienne

SOMMAIRE :

Table des matières

Table des matières

Objectifs :

L'objectif de cette procédure est de configurer un serveur SAMBA avec le protocole LDAP.

Cette procédure à était réalisé pour répondre à un besoin d'une entreprise (CNAM).

J'ai du crée un VM et tout refaire pour pouvoir mettre à jour l'ancien serveur SAMBA.

Le protocole LDAP permettra aux personnels de s'identifier et permettra aussi à notre serveur IPCOP (proxy) de laisser sortir les utilisateurs du réseau si ils ont étaient identifiés par le protocole

Information sur les versions:

VM	Debian 8,2	Jessie	10.19.6.201
	Windows	7	10.19.6.77

Pour cette procédure, nous nous sommes connecté en SSH via un utilisateur puis connexion en tant que root (su)

pour cette procédure, le nom du serveur sera : samba

le mot de passe root sera : root

l'utilisateur de base sera etienne avec le mot de passe : etienne

tout les autres mots de passe seront identique : 12345

le nom du domaine sera : etienne.local

Configuration du serveur :

Configuration du serveur :

Pour commencer, nous devons configurer l'interface de la machine :

```
allow-hotplug eth0
iface eth0 inet static
        address 10.19.6.201
        netmask 255.255.255.0
        gateway 10.19.6.254
```

puis nous mettons à jour la VM :

```
root@samba:~# apt-get update && upgrade_
```

Webmin :

Ensuite, nous allons installer Webmin, pour cela, nous devons le télécharger :

```
root@samba:~# wget http://www.webmin.com/download/deb/webmin-current.deb_
```

```
root@samba:~# apt-get install openssl libauthen-pam-perl libio-pty-perl libnet-s
sleay-perl perl_
```

```
root@samba:~# dpkg --install webmin-current.deb_
```

```
root@samba:~# apt-get -f install_
```

puis nous supprimons le paquet .deb télécharger

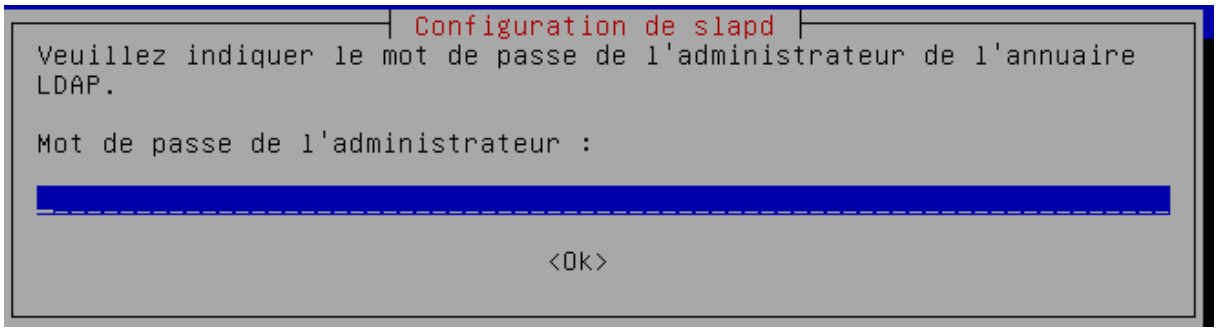
```
root@samba:~# rm webmin-current.deb
```

OpenLDAP : (2.4.40)

Nous allons commencer par télécharger les paquets nécessaires :

```
root@samba:/# apt-get install slapd ldap-utils migrationtools_
```

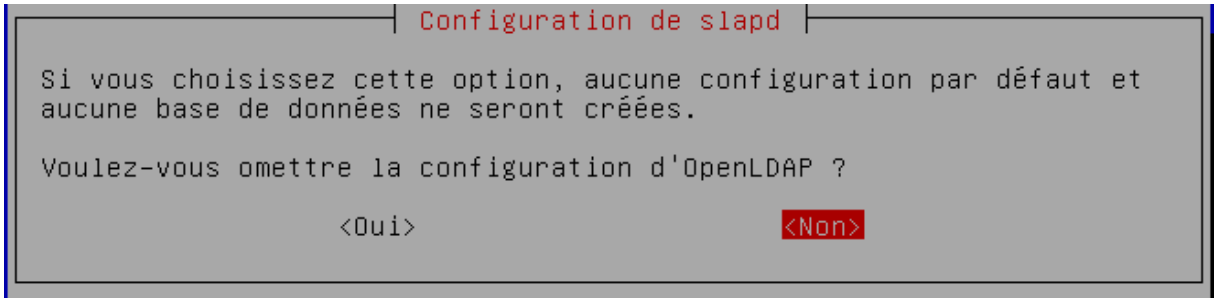
maintenant, vous devez rentrez le mot de passe du super-utilisateur pour l'annuaire LDAP, pour nous le mot de passe sera 12345 :



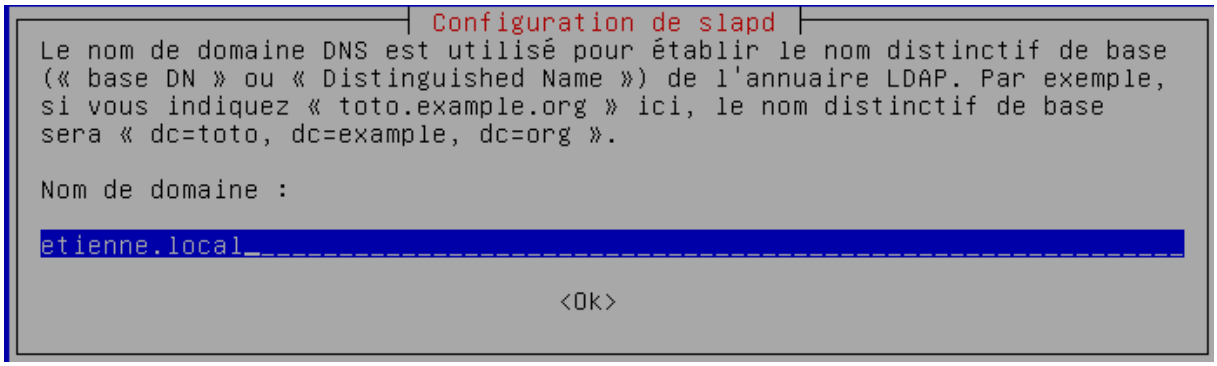
Nous lançons la reconfiguration de slapd :

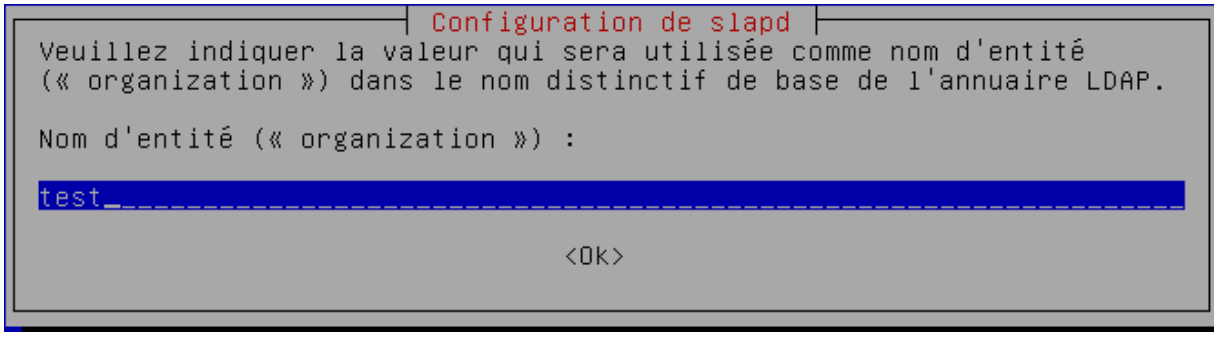
```
dpkg-reconfigure slapd_
```

puis répondez aux questions comme ci-dessous :

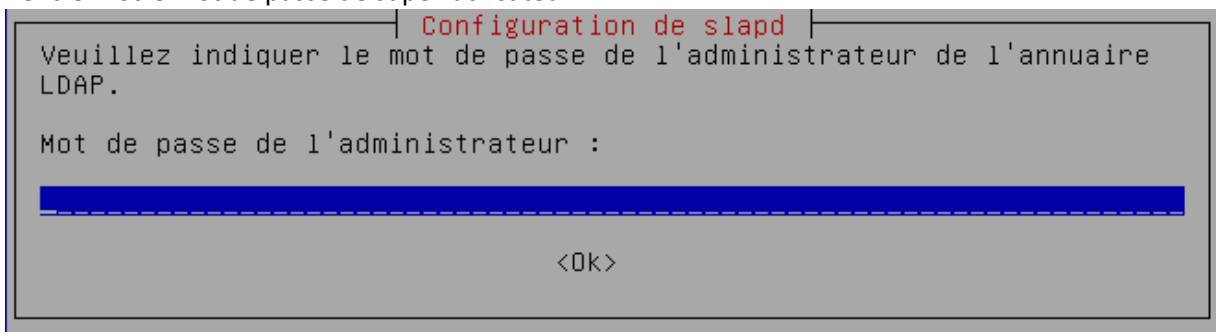


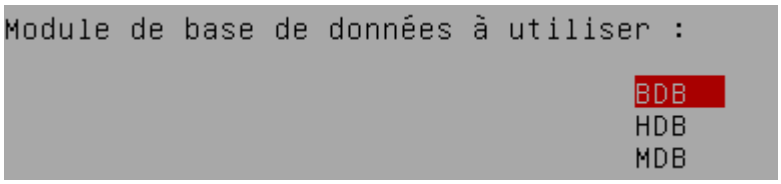
entrez votre nom de domaine :

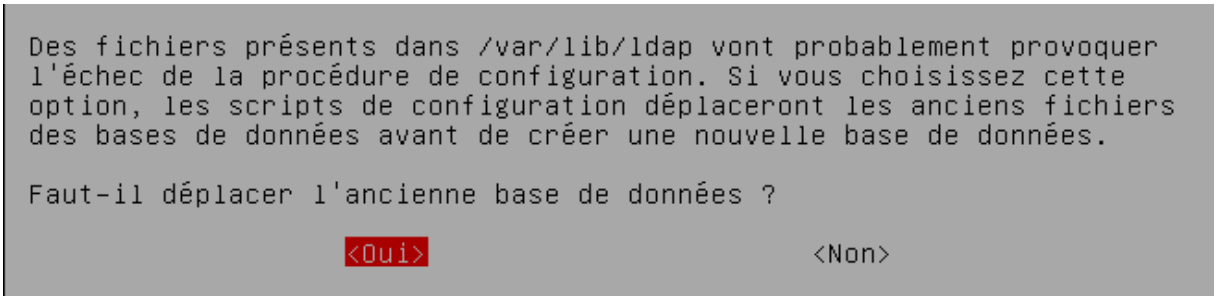


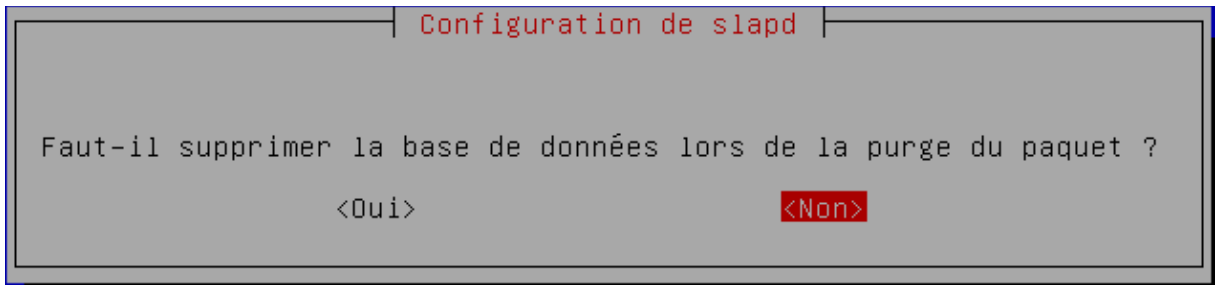


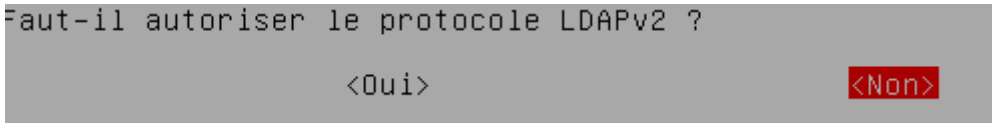
entrez votre mot de passe de super-utilisateur :











Installation de SAMBA :(4.1.17)

Pour l'installation de SAMBA, nous commençons par télécharger les paquets nécessaires :

```
root@samba:/# apt-get install smbldap-tools smbclient samba-doc_
```

```
root@samba:/# apt-get install samba_
```

le paquet samba contient la version 4.1.17 de SAMBA

Liaison SAMBA/LDAP :

```
root@samba:/# cd /etc/ldap_
```

On récupère le schéma SAMBA pour l'insérer dans LDAP

```
root@samba:/etc/ldap# cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
 /etc/ldap/schema_
root@samba:/etc/ldap# gzip -d /etc/ldap/schema/samba.schema.gz
```

Maintenant, nous allons crée le fichier slapd.conf pour pouvoir insérer le schéma SAMBA dans LDAP :

```
root@samba:/etc/ldap# nano slapd.conf_
```

puis écrivez :

```
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/samba.schema
include         /etc/ldap/schema/misc.schema_
```

puis dans le fichier slapd.conf situé en /usr/share/slapd

ajoutez samba.schema et misc.schema a la suite des includes

```
# 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/samba.schema
include         /etc/ldap/schema/misc.schema
```

puis rentrez la commande :

```
root@samba:/etc/ldap# slaptest -f /etc/ldap/slapd.conf -F /etc/ldap/slapd.d_
```

puis :

```
root@samba:/etc/ldap# chown openldap:openldap /etc/ldap/schema/ -R
root@samba:/etc/ldap# chown openldap:openldap /etc/ldap/slapd.d/ -R_
```

ensuite redémarrer le serveur :

```
root@samba:/etc/ldap# reboot_
```

Ensuite, nous allons configurer smb.conf pour la lisaison avec l'annuaire LDAP

```
cd /etc/samba_
```

on fait une sauvegarde du smb.conf :

```
root@samba:/etc/samba# nano smb.conf_ .conf.bckp_
```

puis nous supprimons le fichier smb.conf :

rm smb.conf

puis :

nano smb.conf

```
[global]
#nom du domaine ( à changer en fonction de votre nom de domaine)
        workgroup = LECAUDEY
#nom netbios de votre serveur
        netbios name = samba
#adresse de votre serveur DNS (ici, le serveur DNS est notre serveur samba)
        dns forwarder = 10.19.5.11
        deadtime = 10

#niveau de log, à mettre entre 1 et 3
        log level = 1
#chemin des logs
        log file = /var/log/samba/log.%m
#taille des logs
        max log size = 5000
        debug pid = yes
        debug uid = yes
        syslog = 0
        utmp = yes

#choix de la sécurité
        security = user
#Autorise les scripts
        domain logons = yes
        os level = 64
#lettre de lecteur pour le home
        logon drive = Y:
#adresse du home des utilisateurs (%U renvoie le nom de l'utilisateur connecté)
        logon home = \\samba\%U
#adresse pour les profils itinérants
        logon path = \\samba\profiles\%U
#mettre le nom du script à exécuter (ici, %G renvoie le nom du groupe de l'utilisateur connecté)
        logon script = default.bat

#mettez l'adresse ip de votre serveur LDAP, ici c'est notre serveur donc 127.0.0.1
        passdb backend = ldapsam:"ldap://127.0.0.1/"
#mettre en off lorsque le ssl n'est pas actif
        ldap ssl = off
#veillez mettre votre nom de domaine que vous avez donner lors de l'installation de slapd
        ldap admin dn = cn=admin,dc=etienne,dc=local
        ldap delete dn = no

        ## Sync UNIX password with Samba password
        ## Method 1:
        ldap password sync = yes
        ## Method 2:
        ;ldap password sync = no
        ;unix password sync = yes
```

```
        ;passwd program = /usr/sbin/smbldap-passwd -u '%u'
        ;passwd chat = "Changing *\nNew password*" %n\n "*Retype new password*" %n\n"

#modifiez cette ligne avec le nom de votre domaine
        ldap suffix = dc=etienne,dc=local
        ldap user suffix = ou=Users
        ldap group suffix = ou=Groups
        ldap machine suffix = ou=Computers
        ldap idmap suffix = ou=Idmap
#ici, vous trouverez les scripts pour l'annuaire LDAP
        add user script = /usr/sbin/smbldap-useradd -m '%u' -t 1
        rename user script = /usr/sbin/smbldap-usermod -r '%unew' '%uold'
        delete user script = /usr/sbin/smbldap-userdel '%u'
        set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
        add group script = /usr/sbin/smbldap-groupadd -p '%g'
        delete group script = /usr/sbin/smbldap-groupdel '%g'
        add user to group script = /usr/sbin/smbldap-groupmod -m '%u' '%g'
        delete user from group script = /usr/sbin/smbldap-groupmod -x '%u' '%g'
        add machine script = /usr/sbin/smbldap-useradd -w '%u' -t 1


                create mask = 0666
                directory mask = 0777

                include = /etc/samba/machines/%m.conf

#======= définitions des partages==========#


[homes]
#écriture autorisée
        writeable = yes
#commentaire
        comment = Home Directories
#répertoire de stockage (%U étant le nom de l'utilisateur)
        path = /data/samba/home/%U
#partage caché
        browseable = no
#droit lors de la création de fichiers
        create mask = 0600
#droit lors de la création de dossier
        directory mask = 0700
#authentification est nécessaire
        guest ok = no
```

```
[netlogon]
                comment = netlogon
                path = /data/samba/netlogon
                admin users = root
                guest ok = no
#lecture seule seulement
                read only = yes
                writeable = no
                browseable = no

[profiles]
        comment = Profiles
        path = /data/samba/profiles
        read only = no
        browseable = no
        create mode = 0700

[profiles.V2]
                copy = profiles
```

grâce à la ligne :

```
include = /etc/samba/machines/%m.conf
```

smb.conf utilisera les fichiers %m.conf qui récupere le nom de la machine pour utiliser les fichiers de configurations pour les partages :

exemple pour la machine cnametu21.conf :

```
[partage]
                comment = Partage
                path = /data/partage
                guest ok = no
                browseable = yes
                create mask = 0666
                directory mask = 0777
                read only = no
                valid users = laurent.lecluse,benoit.charles,pannabelle.anglade,@auditeurs,@enseignants
                force group = %G

[divers]
                comment = Divers
                path = /data/divers
                guest ok = no
                browseable = yes
                create mask = 0660
                directory mask = 0770
                read only = no
                valid users = @administratifs
                force group = administratifs

[foad]
                comment = Divers
                path = /data/foad
                guest ok = no
                browseable = yes
                create mask = 0660
                directory mask = 0770
                read only = no
                valid users = @foad
                force group = foad

[documents]
                comment = Documents
                path = /data/documents
                guest ok = no
                browseable = yes
                create mask = 0660
                directory mask = 0770
                read only = no
                valid users = @administratifs
                force group = administratifs
```

Puis nous donnons le mot de passe de l'annuaire LDAP à samba :

```
root@samba:/home/etienne# smbpasswd -w 12345
```

Configuration SMBLDAP-TOOLS :

```
root@samba:/home/etienne# cd /usr/share/doc/smbldap-tools/examples/
root@samba:/usr/share/doc/smbldap-tools/examples# cp smbldap_bind.conf /etc/smbldap-tools/
root@samba:/usr/share/doc/smbldap-tools/examples# cp smbldap.conf.gz /etc/smbldap-tools
root@samba:/usr/share/doc/smbldap-tools/examples# cd /etc/smbldap-tools
root@samba:/etc/smbldap-tools# gzip -d smbldap.conf.gz
root@samba:/etc/smbldap-tools#
root@samba:/etc/smbldap-tools# net getlocalsid
SID for domain SAMBA is: S-1-5-21-343902668-356809154-1294329268
```

Avec cette commande, nous allons récupérer le SID du domaine que nous devons garder pour le mettre dans le fichier smbldap.conf situé dans /etc/smbldap-tools

```
# Put your own SID. To obtain this number do: "net getlocalsid".
# If not defined, parameter is taking from "net getlocalsid" return
SID="S-1-5-21-343902668-356809154-1294329268"
```

sambaDomain »*votre nom de domaine* »

masterLDAP= »ldap://*adresse de votre serveurldap*

ldapTLS= »0 »

suffix= »dc=*etienne*,dc=*local* »

sambaUnixIdPooldn= »sambaDomainName=ETIENNE,${suffix} »

userSmbHome=

userProfile=

userHomeDrive=

userScript

mailDomain= »etienne.local »

ensuite :

```
nano smbldap_bind.conf

masterDN="cn=admin,dc=etienne,dc=local"
masterPw="12345"
```

maintenant, nous mettons les bons droit sur ces fichiers :

```
root@samba:/etc/smbldap-tools# chmod 0644 smbldap.conf
root@samba:/etc/smbldap-tools# chmod 0600 smbldap_bind.conf
```

ensuite, nous allons remplir la base d'annuaire avec quelques entrées Samba et Windows nécessaires :

```
root@samba:/etc/smbldap-tools# smbldap-populate -u 30000 -g 30000
```

Configuration BIND :

```
root@samba:/etc/smbldap-tools# apt-get install bind9
```

Puis dans le fichier named.conf.local dans /etc/bind,

crée une zone primaire :

```
zone "etienne.local" {
        type master;
        file "/var/lib/bind/etienne.local.hosts";
        };
```

et dans le fichier /var/lib/bind/etienne.local.hosts mettez :

```
$ttl 38400
etienne.local.  IN      SOA     samba. root.etienne.local. (
                        1452269018
                        10800
                        3600
                        604800
                        38400 )
etienne.local.  IN      NS      samba.
samba.etienne.local.    IN      A       10.19.6.201
CNAMETU21.etienne.local.        IN      A       10.19.6.77
```

Installation et configuration libnss-ldap et libpam-ldap :

Nous devons installer les paquets :

```
root@samba:/etc/bind# apt-get install libnss-ldap libpam-ldap
```

et repondre aux questions comme ceci :

```
ldap://127.0.0.1
```

```
dc=etienne,dc=local
```

```
3
2
```

```
cn=admin,dc=etienne,dc=local
```

ensuite, rentrez votre mot de passe route et continuez la configuration :

```
Donner les privilèges de superutilisateur local au compte administrateur LDAP ?
                                    <Oui>                                    <Non>
```

```
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>
```

```
Compte de l'administrateur LDAP :

cn=admin,dc=etienne,dc=local
```

et entrez encore une fois votre mot de passe

ensuite, allez dans le fichier nsswitch.conf dans /etc/

et rajoutez :

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

Maintenant, vous pouvez redémarrer votre serveur.

Votre serveur SAMBA et LDAP est prêt, ils ne nous restent plus que à rajouter des utilisateurs, les groupes et ajouter les utilisateurs aux groupes, ensuite, nous finirons par les dossiers partagés avec SAMBA

Création des dossiers SAMBA :

```
root@samba:/home/etienne# mkdir /data
root@samba:/home/etienne# cd /data/
root@samba:/data# mkdir samba
root@samba:/data# mkdir alternance
root@samba:/data# mkdir direction
root@samba:/data# mkdir foad
root@samba:/data# mkdir partage
root@samba:/data# mkdir archivage
root@samba:/data# mkdir divers
root@samba:/data# mkdir horaires
root@samba:/data# mkdir ressources
root@samba:/data# mkdir comptabilite
root@samba:/data# mkdir documents
root@samba:/data# mkdir ingénieurs
root@samba:/data# mkdir samba/netlogon
root@samba:/data# mkdir samba/profiles
root@samba:/data# mkdir samba/home
```

Ensuite, nous créons les groupes avec la commande :

```
root@samba:/data# smbldap-groupadd alternance
root@samba:/data# smbldap-groupadd comptabilite
root@samba:/data# smbldap-groupadd ingenieurs
root@samba:/data# smbldap-groupadd archivage
root@samba:/data# smbldap-groupadd horaires
root@samba:/data# smbldap-groupadd foad
root@samba:/data# smbldap-groupadd auditeurs
root@samba:/data# smbldap-groupadd administratifs
root@samba:/data# smbldap-groupadd enseignants
root@samba:/data# smbldap-groupadd direction
```

ensuite, nous mettons les bons droits sur les dossiers situés dans /data :

chmod 755 /data/samba/home

chmod 755 /data/samba/netlogon

chmod 777 /data/samba/profiles

chmod 770 sur tous les autres dossiers situés dans /data

puis nous donnons la propriété aux groupes auxquels les dossiers appartiennent :

exemple :

```
chown root:direction direction/
chown root:ingenieurs ingénieurs/
chown root:comptabilite comptabilite/
chown root:administratifs documents/
chown root:administratifs divers
chown root:administratifs documents
chown root:foad foad/
chown root:alternance alternance/
chown root:horaires horaires/
chown root:administratifs ressources/
```

ce qui nous donne :

```
drwxr-xr-x 2 root alternance     4096 janv.  8 17:18 alternance
drwxr-xr-x 2 root direction      4096 janv.  8 17:18 direction
drwxr-xr-x 2 root foad           4096 janv.  8 17:18 foad
drwxr-xr-x 2 root root           4096 janv.  8 17:18 partage
drwxr-xr-x 2 root root           4096 janv.  8 17:18 archivage
drwxr-xr-x 2 root administratifs 4096 janv.  8 17:18 divers
drwxr-xr-x 2 root horaires       4096 janv.  8 17:18 horaires
drwxr-xr-x 2 root administratifs 4096 janv.  8 17:18 ressources
drwxr-xr-x 2 root comptabilite   4096 janv.  8 17:18 comptabilite
drwxr-xr-x 2 root administratifs 4096 janv.  8 17:18 documents
drwxr-xr-x 2 root ingenieurs     4096 janv.  8 17:18 ingénieurs
drwxr-xr-x 5 root root           4096 janv.  8 17:18 samba
```

ensuite, nous allons crée des utilisateurs avec la commande :

smbldap-useradd -a -m -s /bin/false -P **nom de l'utilisateur**

cette commande permet d'ajouter un utilisateur à un groupe :

smbldap-groupmod -m **nom de l'utilisateur nom du groupe**

mkdir /data/samba/home/*nom de l'utilisateur*

chown $1:$3 /data/samba/home/*nomdel'utilisateur*

chmod 700 /data/samba/home/*nom de l'utilisateur*

mkdir /data/samba/profiles/*nomdel'utilisateur*.V2

chown *nomdel'utilisateur*:*nomdugroupe* /data/samba/profiles/*nom de l'utilisateur*.V2

chmod 700 /data/samba/profiles/*nom de l'utilisateur*.V2

Installation de phpldapadmin :

```
root@samba:/home/etienne# apt-get install phpldapadmin
```

```
root@samba:/home/etienne# nano /etc/phpldapadmin/config.php
```

Et modifiez les lignes suivantes :

```
$servers->setValue('server','name','10.19.5.11');
```

```
$servers->setValue('server','base',array('dc=etienne,dc=local'));
```

```
$servers->setValue('login','bind_id','cn=admin,dc=etienne,dc=local');
```

puis on déplace le fichier :

cp -R /usr/share/phpldapadmin/ /var/www/phpldapadmin

et maintenant nous pouvons nous connecter à l'adresse suivante :

10.19.5.11/phpldapadmin/

Résolution d'erreur :

Si nous avons des problèmes de jonction au domaine, il faut vérifier les dns

si problème de profils itinérants : vérifiez les droits sur le fichier : profiles dans /data/samba

si problème de script : chmod 777 sur default.bat

chmod u+x default.bat

vérifier le smb.conf

LDAPS :

Nous n'allons pas implémenter de TLS avec le protocole LDAP car le serveur Ip-cop ne le supporte pas