

## Authentification de Samba sous LDAP

Nous allons maintenant configurer Samba, de façon qu'il puisse utiliser le service d'annuaire LDAP pour contenir les informations d'authentification. L'objectif de cette opération est qu'il y ait qu'une seule et unique authentification dans le domaine pour les postes Windows, les postes Linux ainsi que les différents services de notre domaine sous les serveurs.

### Extension du schéma

Avant de débiter, assurez-vous que le fichier *samba.schema* est bien présent dans le répertoire, */etc/openldap/schema/*. Si ce n'est pas le cas, c'est que votre installation d'OpenLDAP n'a pas été correctement effectuée. Vérifier vos USE flags.

Vous avez déjà étendu votre schéma LDAP dans l'unité précédente, en y ajoutant les objets et attributs nécessaires pour Samba. Pour visualiser cette extension, ouvrez le fichier de configuration d'Openldap, *slapd.conf*. A la suite des autres inclusions de schéma, vous devez y retrouver la ligne suivante:

```
...  
include      /etc/openldap/schema/samba.schema
```

Généralement pour vérifier une nouvelle configuration du fichier *slapd.conf* utiliser les commandes suivantes.

```
slaptest
```

```
/etc/init.d/slaped restart
```

NOTES



## Configuration de Samba pour LDAP

Nous allons maintenant ajouter les paramètres de configuration pour que Samba interroge l'annuaire LDAP au lieu de son fichier smbpasswd. Ajouter ces entrées dans le fichier smb.conf dans la section global.

**vim /etc/samba/smb.conf**

```
...
# Parametres pour LDAP.
ldap admin dn = cn=ldapadmin,dc=cybiolab,dc=lan
ldap suffix = dc=cybiolab,dc=lan

passdb backend = ldapsam:ldap://serveurpdc.cybiolab.lan

ldap passwd sync = yes

; ldap machine suffix = ou=Computers
; ldap user suffix = ou=Users
; ldap group suffix = ou=Groups
...
```

Le paramètre *ldap admin dn* est le même que *rootdn* du fichier *slapd.conf*. Il sert à définir le compte qui gère l'annuaire LDAP.

```
ldap admin dn = cn=ldapadmin,dc=cybiolab,dc=lan
```

Le paramètre *ldap suffix* est le même que *suffix* dans le fichier *slapd.conf*. Cette entrée spécifie le DN du suffixe pour les requêtes qui vont être passées à l'annuaire LDAP.

```
ldap suffix = dc=cybiolab,dc=lan
```

Le paramètre *passdb backend* indique la base de données. Nous allons donc indiquer le URL pour rejoindre l'annuaire LDAP.

```
passdb backend = ldapsam:ldap://serveurpdc.cybiolab.lan
```

Actuellement nous utiliserons uniquement LDAP, mais rien ne nous empêcherait d'utiliser plusieurs bases de données contenant les informations d'authentification. Par exemple *smbpasswd* et *ldapsam*.

NOTES



Le prochain paramètre permet à l'utilisateur de pouvoir faire le changement de son mot de passe (`userPassword`) directement de son poste. Cette option nécessite l'ajout du paramètre `password-hash {SSHA}` dans le fichier `slapd.conf`.

`ldap passwd sync = yes`

Valeur	Description
Yes	Lorsque l'utilisateur change son mot de passe, les attributs <code>sambaNTPassword</code> , <code>sambaLMPassword</code> et <code>userPassword</code> sont mis à jour.
No	Lorsque l'utilisateur change son mot de passe, seuls les attributs <code>sambaNTPassword</code> , <code>sambaLMPassword</code> sont mis à jour.

Ici nous vous montrons des paramètres qui ne sont pas vraiment nécessaires si vous utilisez LDAP. Donc inutile de les ajouter.

Comme ces valeurs ne sont pas définies, Samba utilisera la valeur du paramètre `ldap suffix` à la place.

```
; ldap machine suffix = ou=Computers
; ldap user suffix = ou=Users
; ldap group suffix = ou=Groups
```

## Authentification de Samba par LDAP

La commande suivante est utilisée pour spécifier le mot de passe utilisé par le `ldap admin dn`. Le mot de passe sera alors emmagasiné dans le fichier `secrets.tdb` situé dans le répertoire `/var/lib/samba/private/`.

### **smbpasswd -W**

```
Setting stored password for "cn=ldapadmin,dc=cybiolab,dc=lan" in
secrets.tdb
New SMB password:
Retype new SMB password:
```

Faites le test de visualiser son contenu.

```
tdbdump /var/lib/samba/private/secrets.tdb
```

Vous remarquerez qu'en plus du mot de passe du `ldap admin dn`, vous y retrouverez aussi le SID du serveur, ainsi que le SID du

NOTES



