

Procédures d'installation d'OpenLDAP

Installation d'OpenLDAP

L'installation d'écrite dans ce module est celui concernant les contrôleurs de domaine. Pour l'intégration au domaine de contrôleurs de domaine secondaire et de serveurs membres Linux, consulter le module 15. Pour l'intégration de clients Windows et Linux sur le domaine, consulter le manuel *Administrer vos clients sous un domaine Linux* de Cybionet.

Il est à noter que ce n'est pas une obligation d'installer le service OpenLDAP sur le même ordinateur que le service Samba. Par contre, question de simplifier la gestion, nous allons faire suivre ces deux services sur un même ordinateur.

USE Flag	Description
ipv6	Permet le support du IPv6.
kerberos *	Permet le support du MIT Kerberos 5
samba	Permet le support de Samba.
perl *	Permet le support de perl par les scripts Perl.
overlays	Active l'utilisation d'overlays complémentaires.
ssl	Permet le support du LDAPS (TLS).

** Ne sera pas utilisé dans cette version de manuel.*

Si vous ne l'avez pas déjà fait, nous vous conseillons d'ajouter les USE flags directement dans le fichier `/etc/portage/package.use`. Il va permettre d'appliquer ces flags à chaque nouvelle installation ou de les conserver lors de mise à jour d'OpenLDAP.

```
net-nds/openldap -ipv6 samba ssl overlays perl
```

Procédons sans plus attendre à l'installation du service d'annuaire LDAP.

```
emerge -va openldap
```

Une fois l'installation terminée, vérifier qu'OpenLDAP est correctement installé à l'aide de la commande.

```
equery uses openldap
```

NOTES



Configuration d'OpenLDAP 2.3.x

Nous allons maintenant configurer notre serveur LDAP comme maître du domaine. Pour la configuration d'un serveur LDAP esclave, consulter le module 15.



NOTE: Toujours pour les impatientes, consulter immédiatement la totalité des configurations d'OpenLDAP sous l'*Annexe D sous Contrôleur de Domaine Principal*.

NOTES



Édition du fichier de configuration ldap.conf

Il existe deux fichiers de configuration *ldap.conf* sur notre contrôleur de domaine. Chacun d'eux ont leur propre utilité. Le fichier *ldap.conf* situé dans le répertoire */etc/openldap* servira pour le côté serveur de notre contrôleur de domaine alors que le second, situé dans */etc*, servira pour le côté client de notre contrôleur de domaine.

Fichier	Description
<i>/etc/openldap/ldap.conf</i>	<p>Fichier de configuration côté serveur sert pour les services slapd et delta-syncrepl d'OpenLDAP.</p> <p>Ce fichier sera inutile sur les clients Linux avec LDAP. Il est nécessaire uniquement sur les serveurs LDAP.</p> <p>Ce fichier <i>ldap.conf</i> est installé par le paquetage <i>net-nds/openldap</i>.</p>
<i>/etc/ldap.conf</i>	<p>Nécessaire pour le côté client, ce fichier installé par le paquetage <i>sys-auth/nssequ_ldap</i>, contient les informations pour l'identification des serveurs LDAP disponibles et sert en autre pour les services PAM et NSS. N'oublier pas que votre serveur est aussi un client LDAP.</p> <p>Ce fichier est inexistant par défaut sur le poste Linux même avec OpenLDAP d'installé.</p> <p>Ce fichier <i>ldap.conf</i> est installé par le paquetage <i>sys-auth/nss_ldap</i>.</p>

Dans les pages suivantes, nous allons configurer les deux fichiers `ldap.conf` de façon indépendants. Dans certain cas avoir le même fichier peut occasionner des troubles.

Le fichier de configuration `ldap.conf` que nous allons configurer se retrouve dans le répertoire `/etc/openldap/`. Celui donc du **côté serveur** de notre contrôleur de domaine.

```
vim /etc/openldap/ldap.conf
```

Identification du serveur d'annuaire LDAP

```
BASE dc=cybiolab,dc=lan
URI ldap://serveurpdc.cybiolab.lan
...
```

Le paramètre `base` vous permettra de définir la base du domaine par défaut lorsqu'une opération quelconque sera effectuée sur l'annuaire LDAP. La base doit être spécifiée comme un nom unique (DN) en format LDAP.

```
BASE dc=cybiolab,dc=lan
```

Le paramètre `URI` (*Uniform Resource Identifier*) d'un serveur LDAP défini à quel annuaire LDAP doit se connecter. Si vous désirez spécifier plusieurs entrées (exemple pour un BDC), un espace est nécessaire pour séparer la liste des URI.

```
URI ldap://serveurpdc.cybiolab.lan
```

Caractéristiques du serveur d'annuaire LDAP

```
...
rootbinddn cn=ldapadmin,dc=cybiolab,dc=lan
scope one
ldap_version 3
...
```

```
rootbinddn cn=ldapadmin,dc=cybiolab,dc=lan
```

Le paramètre `rootbinddn` vous permettra d'indiquer l'utilisateur "ldapadmin" (*manager*) qui se connectera à votre annuaire LDAP.

NOTES



Identification et caractéristiques du client LDAP

Réinscrivez l'identification et caractéristiques du serveur LDAP que nous venons de voir dans le fichier `ldap.conf`. Prenez soin de mettre l'entrée `rootbinddn` en commentaire.

```
BASE dc=cybiolab,dc=lan
URI ldap://serveurpdc.cybiolab.lan

scope one
ldap_version 3
...
```



ATTENTION: Le paramètre `rootbinddn` ne devrait jamais être utilisée sur la section cliente Linux de LDAP.

Configuration des paramètres PAM du client LDAP

Nous allons voir au prochain module ce mécanisme d'authentification. Pour l'instant, nous nous contenterons de savoir que ces entrées permettent de configurer les paramètres PAM pour le côté client LDAP de notre serveur.

```
...
# Paramètres pour PAM.
pam_filter objectclass=posixAccount
pam_login_attribute uid
pam_member_attribute memberuid
pam_password exop

bind_policy soft
...
```

Le paramètre `pam_filter`, fait un filtre pour permettre la recherche dans l'annuaire LDAP qu'aux objets qui possèdent un attribut `posixAccount`.

```
pam_filter objectclass=posixAccount
```

Définissons l'attribut d'identification unique des comptes authentifiés, généralement il s'agit de l'attribut `uid`.

```
pam_login_attribute uid
```

NOTES



Configuration des paramètres NSS du client LDAP

Tous comme le mécanisme d'authentification PAM, que nous allons voir au prochain module, nous allons nous contenter de configurer le service LDAP pour NSS.

vim /etc/ldap.conf

```
...
# Paramètres pour NSS.
nss_base_passwd dc=cybiolab,dc=lan
nss_base_shadow dc=cybiolab,dc=lan

nss_base_passwd ou=Users,dc=cybiolab,dc=lan?sub
nss_base_shadow ou=Users,dc=cybiolab,dc=lan?sub

nss_base_group ou=Groups,dc=cybiolab,dc=lan?sub
nss_base_hosts ou=Computers,dc=cybiolab,dc=lan
nss_base_hosts ou=DomainControllers,dc=cybiolab,dc=lan
```

Les entrées *nss_base_passwd* et *nss_base_shadow* vont permettre d'indiquer où se trouve les attributs pour l'authentification au niveau de cybiolab.lan seulement (*one*).

```
nss_base_passwd dc=cybiolab,dc=lan
nss_base_shadow dc=cybiolab,dc=lan
```

Ces secondes entrées *nss_base_passwd* et *nss_base_shadow* vont permettre d'indiquer où se trouve les attributs pour l'authentification des utilisateurs du domaine. Donc ici les informations se retrouveront dans *ou=Users,dc=cybiolab,dc=lan* et ses sous-entrées.

```
nss_base_passwd ou=Users,dc=cybiolab,dc=lan?sub
nss_base_shadow ou=Users,dc=cybiolab,dc=lan?sub
```

Nous indiquons maintenant où se situent les attributs pour les groupes du domaine.

```
nss_base_group ou=Groups,dc=cybiolab,dc=lan?sub
```

NOTES

Nous indiquons maintenant où se situent les informations pour les ordinateurs du domaine et contrôleurs de domaine.

```
nss_base_hosts ou=Computers,dc=cybiolab,dc=lan
nss_base_hosts ou=DomainControllers,dc=cybiolab,dc=lan
```



NOTE: Ici encore, nous limiterons l'utilisation de la plage de recherche sub pour les performances. Contentez-vous de l'appliquer qu'aux entrées `nss_base_passwd`, `nss_base_shadow` et `nss_base_group` seulement.

NOTES



Édition du fichier de configuration slapd.conf

Le fichier de configuration `slapd.conf` va vous permettre de définir la configuration des services ldap (`slapd`). Ce fichier sert uniquement pour les serveurs hébergeant le service d'annuaire LDAP. Donc il est inutile de le configurer sur les serveurs membres ou les postes clients Linux.

Définition du schéma

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema
...
```

Ces entrées vont nous permettre de configurer les schémas que supportera notre annuaire LDAP. Le simple fait d'ajouter une entrée `include` va étendre le schéma, et l'inverse, la suppression d'une entrée incluse va réduire notre schéma. Rien à voir avec Active Directory n'est-ce pas ?

L'ordre d'application des schémas est très important, car chacun des classes d'objets dépend de d'autres classes ou attributs qui doivent exister. Par exemple, le schéma `"core"` contient la classe `"top"` qui est celle dont tous les schémas dépendent. Il sera donc chargé en premier.

Les fichiers des schémas sont situés dans le répertoire `/etc/openldap/schema/`. Voici un tableau contenant une très brève description des différents schémas ainsi que leur RFC s'y rattachant, si vous voulez en savoir plus.

Schéma	Description	RFC
core	Fichier de schéma minimal à inclure dans votre service d'annuaire LDAP. Il permet de définir les attributs de bases de LDAPv3 conformément aux RFC suivants.	RFC1274 RFC2079 RFC2247 RFC2251 RFC2252 RFC2253 RFC2254 RFC2255 RFC2256 RFC2377 RFC2589
cosine	Support des annuaires COSINE et X.500.	RFC1274
inetorgperson	Permet de définir des informations sur les utilisateurs et différents objets.	RFC2798
nis	Schéma nécessaire pour remplacer NIS par LDAP.	RFC2307 RFC2252

Définition du schéma

```
...
pidfile      /var/run/openldap/slapd.pid
argsfile     /var/run/openldap/slapd.args

allow bind_v2

password-hash {SSHA}
password-crypt-salt-format "$1$%.8s"

modulepath /usr/lib/openldap/openldap
moduleload back_hdb.so
...
```

```
pidfile      /var/run/openldap/slapd.pid
argsfile     /var/run/openldap/slapd.args
```

NOTES



Plusieurs entrées de suffixe peuvent être données, mais au moins une entrée est nécessaire pour chacune des définitions de base de données.

```
suffix      "dc=cybiolab,dc=lan"
```

Cette entrée définit le DN du compte `ldapadmin` (*manager*) pour l'annuaire LDAP. Le DN spécifié dans cette entrée ne sera pas sujet aux ACLs définis dans le `slapd.conf` ou à aucune autre restriction administrative sur les opérations sur la base de données.

```
rootdn      "cn=ldapadmin,dc=cybiolab,dc=lan"
```

L'entrée suivante permet de définir le mot de passe pour l'entrée DN spécifié par le `rootdn`. Les types hachages acceptés sont les mêmes que décrit dans le RFC 2307, soit: MD5, SMD5, Crypt, SHA, SSHA. Le mot de passe peut aussi être entré en texte clair (utile pour l'expérimentation dans un environnement de test seulement).

```
rootpw {SSHA}sk5O6v7RwZHjsVU9aIFgHfkG/4qqbjik
```

Pour générer votre mot de passe crypté, ouvrir une console et utiliser la commande `slappasswd`

Syntaxe:

```
slappasswd -h {type_de_hachage}
```

Par exemple:

```
slappasswd -h {SSHA}  
New password:  
Re-enter new password:  
{SSHA}sk5O6v7RwZHjsVU9aIFgHfkG/4qqbjik
```

Indexation de l'annuaire LDAP

L'indexation permet de réduire les requêtes d'objets à l'annuaire LDAP. Quoique cela semble simple et laisse miroiter de belle hausse de performance, une mauvaise utilisation ou configuration entraînera une baisse flagrante de performance voire même un arrêt complet du service LDAP. Nous allons nous contenter du minimum ce qui devrait répondre à tous les besoins d'entreprise.

```
index objectClass eq
```

NOTES



Afin d'améliorer les performances d'OpenLDAP pour le soutien de Samba, ajouter immédiatement les entrées suivantes. Nous le faisons immédiatement, car l'ajout de ces lignes une fois l'annuaire LDAP créé est extrêmement compliqué et entraîne une dégradation majeure en cas d'erreur.

```
...
index sambaSID,SambaSIDList,sambaPrimaryGroupSID eq
index sambaGroupType eq
index sambaDomainName eq
index uid,uidNumber,gidNumber,uniqueMember,memberUid eq
index cn,mail,surname,givenName eq,subinitial
```

Configuration pour la base de donnée

Ce fichier de configuration est uniquement utilisé avec les bases de donnée BDB et HDB. Laissez le tel quel.

```
cd /var/lib/openldap-data/
cp DB_CONFIG.example DB_CONFIG
```

NOTES



Initialisation

Vous voilà donc avec un annuaire LDAP fonctionnel, qui n'est pas sécuritaire pour l'instant, qui ne génère pas d'audit et qui ne supporte pas encore Samba. Patience, l'installation de votre contrôleur de domaine est presque terminée. Ne reste plus qu'à initialiser le service d'annuaire LDAP.

Démarrer le service OpenLDAP

Le service OpenLDAP porte le nom de *slapd*. Donc pour exécuter la section serveur d'OpenLDAP, saisissez la commande suivante:

```
/etc/init.d/slapd start
```

Scripts d'initialisation

Votre service d'annuaire LDAP est démarré, mais elle ne contient pas encore de base de données. Nous allons donc initialiser une nouvelle BD. Mais avant de lancer le script de la création du rootdn, assurez-vous que le service est bien démarré.

```
/etc/init.d/slapd status  
* status: started
```

Le script bash suivant va nous permettre d'ajouter les informations de notre domaine et sur notre administrateur d'annuaire qui sont contenu dans un fichier au format LDIF.

Créez un fichier portant le nom **import_ldif.sh** et inscrivez-y les lignes suivantes. Modifier l'entrée de la variable ROOTDN afin de la personnaliser selon votre propre *rootdn*.

```
#!/bin/bash
# *****
# * Auteur:      Robert Descôteaux
# * Création:   Cybionet
# *
# * Fichier:     import_ldif.sh
# * Version:    1.0.2
# *
# * Commentaire: Ce script permet de réimporter les informations
# * contenu dans un fichier au format LDIF dans l'annuaire LDAP
```

NOTES



```
# * suite à une mise à niveau d'OpenLDAP.
# *
# * Date: 20 octobre 2007
# * Modification: 03 mars 2010
# * *****

# Configuration de votre rootdn.
ROOTDN="cn=ldapadmin,dc=cybiolab,dc=lan"

# Message d'utilisation du script.
if test $# -eq 0; then
  echo "Cybionet - Solution reseautique"
  echo "-----"
  echo " "
  echo usage: `echo $0 | sed 's,^.,,,' "fichier.ldif"
  echo " "
  exit 1
fi

# Commande d'ajout du fichier LDIF
/usr/bin/ldapadd -x -D "$ROOTDN" -W -f $1
```

Ce script peut être récupérer pour importer tout vos fichiers LDIF dans votre annuaire LDAP de votre serveur.

Décortiquons les commutateurs passés avec la commande *ldapadd*.

Commutateurs	Description
-f	Indique le nom du fichier de modification (LDIF) contenant les entrées pour l'annuaire LDAP.
-x	Utilise une authentification simple au lieu du mécanisme SASL.
-D	Indique le DN du binddn pour accéder à l'annuaire LDAP.
-W	Demande le mot de passe pour l'authentification. Cela évite de devoir entrer le mot de passe directement dans la commande avec le commutateur -w.

Changer les permissions sur le script afin qu'il soit exécutable.

```
chmod 700 import_ldif.sh
```

NOTES



Les fichiers au format LDIF (*LDAP Data Interchange Format*) défini par le RFC2849 permettent d'effectuer des modifications par lot dans l'annuaire LDAP. Il s'agit d'un simple fichier ASCII qui peut être édité à l'aide de vos éditeur texte préféré (vi, nano, notepad ou encore wordpad).

Ce format est standard pour tout les annuaires, il va nous faciliter la vie pour créer des utilisateurs/groupes, faire la migration des utilisateurs d'Active Directory vers OpenLDAP ou encore récupérer notre arborescence suite à une erreur humaine.

Créer un fichier portant le nom `init_srv.ldif` et inscrivez-y les lignes suivantes.

```
dn:dc=cybiolab,dc=lan
objectclass: dcObject
objectclass: organization
o: Cybiolab
dc: cybiolab

dn:cn=ldapadmin,dc=cybiolab,dc=lan
objectclass: organizationalRole
cn:ldapadmin
```

Le premier bloc d'entrée sous le DN `dc=cybiolab,dc=lan`, défini votre domaine. Personnaliser donc les entrées `dn`, `o` et `dc` selon vos besoins.

Le second bloc correspond à l'entrée `rootdn`. Il est important qu'il soit identique au nom entré dans le fichier `slapd.conf`.

Exécuter le script bash.

```
./import_ldif.sh init_srv.ldif
```

Lors de l'exécution du script, vous devrez avoir le message suivant:

```
Enter LDAP Password:
adding new entry "dc=cybiolab,dc=lan"

adding new entry "cn=ldapadmin,dc=cybiolab,dc=lan"
```

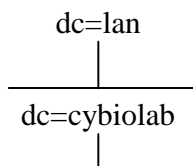
NOTES



Création de la structure DIT

Dans l'unité 1 de ce module, nous vous avons présenté une structure DIT de base qui vous permettra de développer selon les besoins de votre entreprise.

Actuellement votre structure devrait ressembler à ceci.



Comme vous pouvez le constater il vous manque une grande partie de la structure DIT initialement prévue.

Créer un fichier portant le nom **baseDIT.ldif** et inscrivez-y les lignes suivantes.

```

dn: ou=Computers,dc=cybiolab,dc=lan
ou: Computers
objectClass: top
objectClass: organizationalUnit
description: Default container for computer accounts

dn: ou=Domain Controllers,dc=cybiolab,dc=lan
ou: Domain Controllers
objectClass: top
objectClass: organizationalUnit
description: Default container for domain controllers

dn: ou=Groups,dc=cybiolab,dc=lan
ou: Groups
objectClass: top
objectClass: organizationalUnit
description: Default container for groups

dn: ou=System,ou=Groups,dc=cybiolab,dc=lan
ou: System
objectClass: top
objectClass: organizationalUnit

dn: ou=Users,dc=cybiolab,dc=lan
ou: Users
objectClass: top
objectClass: organizationalUnit
description: Default container for users accounts
  
```

NOTES



```
dn: ou=System,ou=Users,dc=cybiolab,dc=lan
ou: System
objectClass: top
objectClass: organizationalUnit
```

```
dn: ou=Services,dc=cybiolab,dc=lan
ou: Services
objectClass: top
objectClass: organizationalUnit
description: Default container for services
```

Encore une fois, faites l'importation de votre fichier LDIF. Pour ce faire exécuter le script bash `import_ldif.sh` précédemment crée.

```
./import_ldif.sh baseDIT.ldif
```

Vérification des configurations

Il est important de vérifier la configuration du fichier `slapd.conf` lorsque vous faites une modification dans ce dernier avant de l'appliquer. Pour faire cette vérification, utiliser la commande `slaptest`.

```
slaptest
```

Vous devriez obtenir le résultat:

```
config file testing succeeded
```



NOTE: Si vous utilisez la base de données de type LDBM, vous allez obtenir l'erreur suivante:

```
WARNING: No dynamic config support for database ldbm.
ldb_m_back_db_open: database already in use
backend_startup_one: bi_db_open failed! (-1)
slap_startup failed (test would succeed using the -u switch)
```

Utiliser à la place la commande `slaptest -u`, et penser à planifier une migration vers le type de base de données BDB ou HDB.

NOTES



Nous allons maintenant faire une demande à l'annuaire LDAP, question de voir s'il répond correctement. Dans une console saisissez.

```
ldapsearch -x -h serveurpdc.cybiolab.lan -D cn=ldapadmin,dc=cybiolab,dc=lan -W
```

Vous devriez obtenir le résultat suivant.

```
# extended LDIF
#
# LDAPv3
# base <> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# cybiolab.lan
dn: dc=cybiolab,dc=lan
objectClass: dcObject
objectClass: organization
o: Cybiolab
dc: cybiolab
# ldapadmin, cybiolab.lan
dn: cn=ldapadmin,dc=cybiolab,dc=lan
objectClass: organizationalRole
cn: ldapadmin
# Computers, cybiolab.lan
dn: ou=Computers,dc=cybiolab,dc=lan
ou: Computers
objectClass: top
objectClass: organizationalUnit
description: Default container for computer accounts
# Domain Controllers, cybiolab.lan
dn: ou=Domain Controllers,dc=cybiolab,dc=lan
ou: Domain Controllers
objectClass: top
objectClass: organizationalUnit
description: Default container for domain controllers
# Groups, cybiolab.lan
dn: ou=Groups,dc=cybiolab,dc=lan
ou: Groups
objectClass: top
objectClass: organizationalUnit
description: Default container for groups
# System, Groups, cybiolab.lan
dn: ou=System,ou=Groups,dc=cybiolab,dc=lan
ou: System
```

NOTES



```
objectClass: top
objectClass: organizationalUnit

# Users, cybiolab.lan
dn: ou=Users,dc=cybiolab,dc=lan
ou: Users
objectClass: top
objectClass: organizationalUnit
description: Default container for users accounts

# System, Users, cybiolab.lan
dn: ou=System,ou=Users,dc=cybiolab,dc=lan
ou: System
objectClass: top
objectClass: organizationalUnit

# Services, cybiolab.lan
dn: ou=Services,dc=cybiolab,dc=lan
ou: Services
objectClass: top
objectClass: organizationalUnit
description: Default container for services

# search result
search: 2
result: 0 Success

# numResponses: 10
# num Entries: 9
```

Si cela ne fonctionne pas, essayer plutôt avec une adresse IP afin d'isoler le problème de résolution de nom DNS.

Idapsearch -x -h 192.168.0.2 -D cn=ldapadmin,dc=cybiolab,dc=lan -W

Si cela ne fonctionne toujours pas, assurez-vous que votre service slapd est bien démarré et vérifiez de nouveau les entrées dans le fichier ldap.conf du côté serveur, soit dans le répertoire /etc/openldap/.

Il est important que tout cela fonctionne correctement avant de poursuivre l'installation de votre serveur.

NOTES

