

OpenLDAP, un outil d'administration Réseau

Une implémentation d'OpenLDAP

INRA de Rennes

UMR-118

**Amélioration des Plantes
et Biotechnologies Végétales**

Présentation :

Lightweight Directory Access Protocol

- Allègement du protocole X500,
- Manipulation des annuaires réseaux,
- Suivi des RFC,
- Standard actuel.

Les Annuaires LDAP :

Les versions commerciales :

Novell : NDS, Netware Directory Services
E-directory

SUN-Netscape : I-Planet,

Microsoft : Active Directory Services.

Et

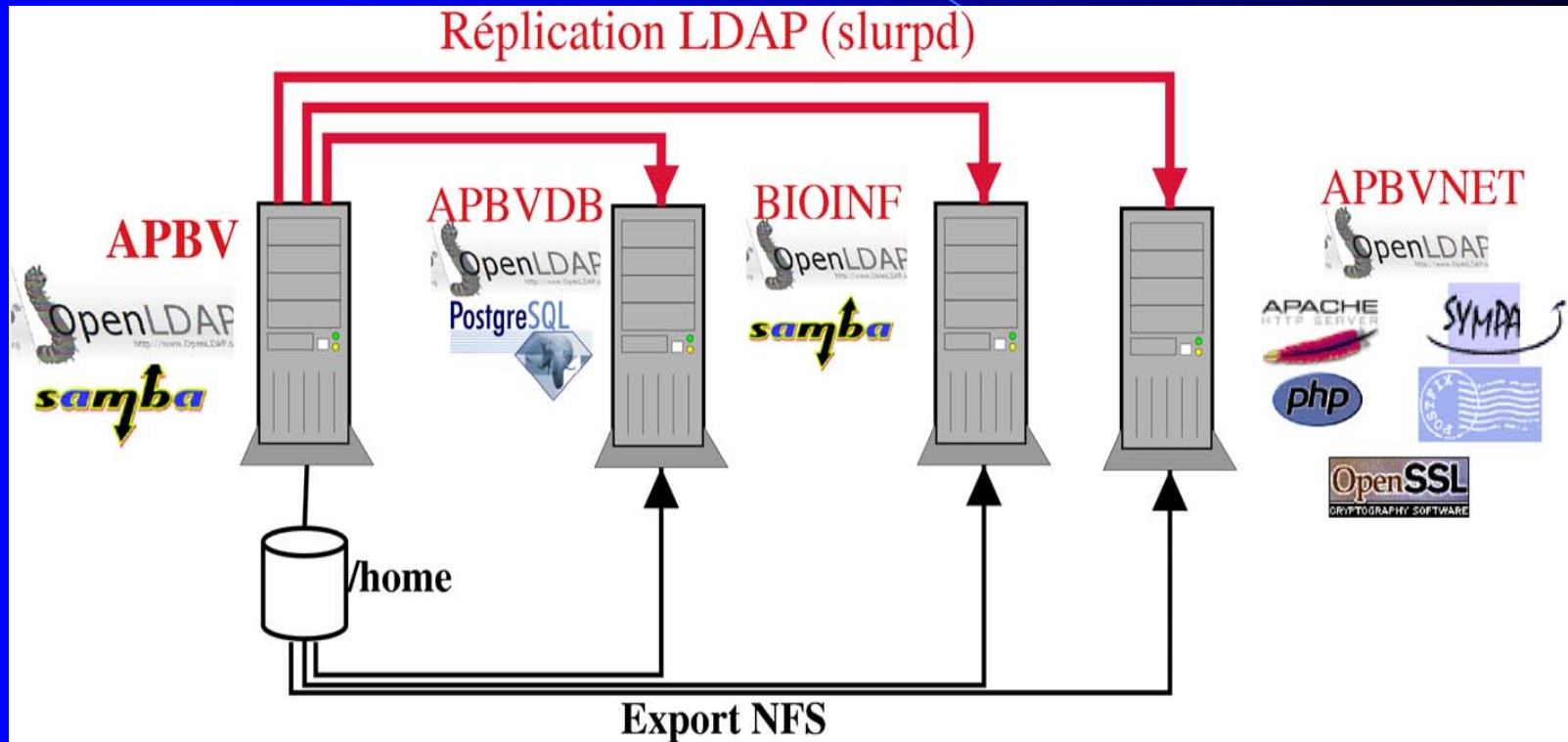
OpenLDAP :

Version actuelle : 2.1.23

Fonctionnalités attendues :

- **Gestion des comptes utilisateurs et Authentification centralisées,**
- **Base de données utilisateurs et machines,**
- **Accessibilité multi-OS,**
- **Compatibilité multi-logiciels.**

Organisation matérielle Et logicielle :



logiciels utilisés :

- **Serveur Linux Debian (3.0) Woody,**
 - **Ldap 2.0.18,**
 - **Samba 2.2.5,**
 - **Postfix,**
 - **Sympa 3.4.4.1,**
 - **Apache 1.3.28 + PHP4.3.3**
 - **OpenSSL 0.9.6.**

Architecture Réseau-Serveurs :

- 1 Serveur Maître LDAP + Samba
- 3 serveurs esclaves LDAP dont :
 - Serveur web apache + sympa + openssl,
 - Serveur de base de données PostgreSQL, ...
 - Serveur d'applications Bio-informatiques.

Installation :

Bibliothèques : libpam-ldap,
libnss-ldap,
libldap2 + dev,

Démons : slapd,
slurpd,

Cryptographie : openssl,
sasl,

Outils : ldap-utils.

Paramétrages LDAP :

Fichier de configuration :

`~/etc/openldap/slapd.conf,`

- définition des schémas et classes d'objets,
- définition du backend,
- définition de la base de l'annuaire et du compte admin,
- définition des réplicats,
- définitions des ACLs,
- ...

Les schémas LDAP :

Fichier slapd.conf

Directive : include /path/vers/fichier.schema

- Ensemble d'objets définis par un oid,
- les objets sont définis par des attributs,
- les attributs sont obligatoires ou optionnels,
- extensions des schémas à volonté.

Schémas :

Répertoire d'installation :

~/etc/openldap/schemas,

Les schémas installés et déclarés vont déterminer les objets utilisables pour votre annuaire.

Il faut donc récupérer ceux qui conviennent.

En général ils sont fournis avec les sources ;

ex : samba.schema ;

Le choix du schéma d'annuaire est primordial.

Ici un compte users est l'association de 7 objets.

Schémas :

The screenshot shows the GQ (Gestionnaire de Qualité) interface. The window title is "GQ". The menu bar includes "File", "Filters", and "Help". The main area has three tabs: "Search", "Browse", and "Schema". The "Schema" tab is active, showing a tree view on the left and a detailed view on the right.

Tree View:

- apbv
 - objectClasses
 - account**
 - alias
 - applicationEntity
 - applicationProcess
 - automount
 - automountMap
 - bootableDevice
 - certificationAuthority
 - certificationAuthority-V2
 - country
 - cRLDistributionPoint
 - dcObject
 - device
 - dmd
 - dNSDomain
 - document
 - documentSeries
 - domain

Objectclasses View:

Objectclasses	Attribute types	Matching rules	Syntaxes
Name	account	Required attributes	userid
Description		Allowed attributes	description seeAlso localityName organizationName organizationalUnitName host
OID	9.2342.19200300.100.4.5		
Superior	top		
Kind	Structural		
	<input type="checkbox"/> Obsolete		

Schema search on cn=Subschema

Paramétrages LDAP : Fichier slapd.conf

Backend :

- moteur de base de données de l'annuaire local :
- directive : database
 - ldbm (standard),
 - berkeleyDB, (sleepycat),
 - SQL,
 - LDAP (méta-annuaire).

Paramétrages LDAP : Fichier slapd.conf

Base de l'annuaire :

Suffix : racine de l'arbre (là où va commencer l'annuaire)
ici : "o=inra,c=fr"

rootdn : c'est l'administrateur de l'annuaire local
cn=root,o=inra,c=fr,

rootpw : mot de passe de l'admin.

Paramétrages LDAP : Fichier slapd.conf

Directives de réplication :

Maître :

repllogfile : fichier où slapd va enregistrer les modifications pour slurpd,

replica : host = serveur ldap : 389
binddn= administrateur de l'annuaire
bindmethod = simple, sasl ...
credentials = mot de passe de l'admin.

Esclave :

updatedn : "administrateur de l'annuaire"
updateref : ldap://serveur LDAP Maître : 389

Paramétrages LDAP : Fichier slapd.conf

les ACLs (Access Lists) :

dans le fichier slapd.conf

gestion de droits d'accès aux données de LDAP
par défaut : lecture sur tout en « anonyme »

Les acls par défaut :

access to *

by self write

by users read

by anonymous auth .

Un bind nécessite un accès en lecture de l'annuaire.

Déploiement de l'annuaire

Annuaire : Structure arborescente

Choix des objets :

Les objets conteneurs : OrganizationalUnit,

Les objets feuilles : Account, Device etc ..

Associations d'objets :

un utilisateur, un ordinateur.

Entités définies par un DN unique.

Déploiement de l'annuaire

Premières entrées fichier LDIF :

dn: o=inra,c=fr
objectClass: top
objectClass: organization
o: inra
description: Institut National de la Recherche Agronomique
businessCategory: EPST

dn: ou=rennes,o=inra,c=fr
objectClass: top
objectClass: organizationalUnit
ou: rennes
street: Domaine de la Motte
postalCode: 35653
postalAddress: Le Rheu Cedex
l: Rennes
st: Ile et vilaine
postOfficeBox: 35327
businessCategory: Centre de Recherche INRA de Rennes
description: Centre de Recherche INRA de Rennes

Commande Idapadd.

Déploiement de l'annuaire

Vue générale de l'arborescence:

The screenshot shows a directory browser window with a tree view on the left and a details pane on the right. The tree view shows a hierarchy starting with 'o=inra,c=fr' and including various organizational units (ou) and users (cn). The details pane shows the following information:

dn	o=inra,c=fr
objectClass	top
	organization
o	inra
userPassword	<input type="text"/> Clear
searchGuide	<input type="text"/>
seeAlso	<input type="text"/>
businessCategory	EPST
x121Address	<input type="text"/>
registeredAddress	<input type="text"/>
destinationIndicator	<input type="text"/>
preferredDeliveryMethod	<input type="text"/>
telexNumber	00 00 00 00
teletexTerminalIdentifier	<input type="text"/>
telephoneNumber	<input type="text"/>
internationalISDNNumber	<input type="text"/>
facsimileTelephoneNumber	<input type="text"/>

Buttons: Apply, Refresh

Déploiement de l'annuaire

Vue d'un objet conteneur OrganizationalUnit :

The screenshot shows a LDAP browser window with a tree view on the left and a details pane on the right. The tree view shows a hierarchy starting with 'o=inra,c=fr' and a sub-tree for 'ou=rennes'. The details pane shows the following attributes and values:

dn	ou=rennes,o=inra,c=fr
objectClass	top
	organizationalUnit
ou	rennes
userPassword	<input type="text"/> Clear
searchGuide	
seeAlso	
businessCategory	Centre de Recherche INRA
x121Address	
registeredAddress	rennes
destinationIndicator	
preferredDeliveryMethod	
telexNumber	00 00 00

At the bottom of the window, there is an 'Apply' button and a 'Refresh' button. The status bar at the bottom of the window displays 'modified ou=rennes,o=inra,c=fr'.

Déploiement de l'annuaire

Vue d'un objet feuille : PosixGroup

The screenshot shows the GQ LDAP browser interface. On the left, a tree view displays the LDAP hierarchy, with the object 'cn=aqr' selected under 'ou=groups'. The right pane shows the details for this object:

dn	cn=aqr,ou=groups,ou=apbv,ou=lerheu,ou=...	
objectClass	top	<input checked="" type="checkbox"/>
	posixGroup	<input checked="" type="checkbox"/>
cn	aqr	<input checked="" type="checkbox"/>
gidNumber	250	
userPassword	<input type="text" value=""/>	<input checked="" type="checkbox"/>
	<input type="button" value="Clear"/>	
memberUid	esnault	
	lassalle	
	vallee	
	abelard	
	bregeon	
	jahier	
	launay	
	...	

Buttons for 'Apply' and 'Refresh' are visible at the bottom of the details pane.

Déploiement de l'annuaire

Vue d'un compte machine :

The screenshot shows a LDAP browser window with a tree view on the left and a details pane on the right. The tree view shows a hierarchy starting from 'apbv' down to 'ou=computers' and finally 'cn=abioinf1'. The details pane shows the following attributes:

dn	cn=abioinf1,ou=computers,ou=apbv,ou=lerheu,ou=ren
objectClass	top device ipHost account posixAccount sambaAccount
cn	abioinf1
serialNumber	
seeAlso	
owner	cn=Stephane NICOLAS
ou	
o	
l	
description	
ipHostNumber	194.254.140.211
manager	cn=Gilles LASSALLE

At the bottom of the window, the text reads: modified cn=abioinf1,ou=computers,ou=apbv,ou=lerheu,ou=rennes,o=inra,c=fr

Déploiement de l'annuaire

Vue d'un objet OrganizationalRole :

The screenshot shows a LDAP browser window with a tree view on the left and a details pane on the right. The tree view shows a hierarchy starting with 'apbv' and 'ou=rennes', with 'cn=President' selected. The details pane shows the following attributes:

Attribute	Value	Checkmark
dn	cn=President,ou=rennes,o=inra,c=fr	
objectClass	top	<input checked="" type="checkbox"/>
	organizationalRole	<input checked="" type="checkbox"/>
cn	president	<input checked="" type="checkbox"/>
x121Address		<input checked="" type="checkbox"/>
registeredAddress		<input checked="" type="checkbox"/>
destinationIndicator		<input checked="" type="checkbox"/>
preferredDeliveryMethod		
telexNumber		<input checked="" type="checkbox"/>
teletexTerminalIdentifier		<input checked="" type="checkbox"/>
telephoneNumber		<input checked="" type="checkbox"/>
internationalISDNNumber		<input checked="" type="checkbox"/>
facsimileTelephoneNumber		<input checked="" type="checkbox"/>
seeAlso		<input checked="" type="checkbox"/>
roleOccupant	cn=Gerard MAISSE	<input checked="" type="checkbox"/>

Buttons: Apply, Refresh

no entries found (finished)

LDAP et la réplication : description

**-2 types de serveurs :
Maître et esclave**

**-2 démons :
SLAPD et SLURPD**

-Maître : Slapd + Slurpd

-Esclave : Slapd

LDAP et la réplication : Mécanisme

-Slapd + directive relogfile

→ création du fichier des modifications pour slurpd

-Slurpd :

-lecture des informations du *relogfile*,

-lecture des directives replica dans le slapd.conf,

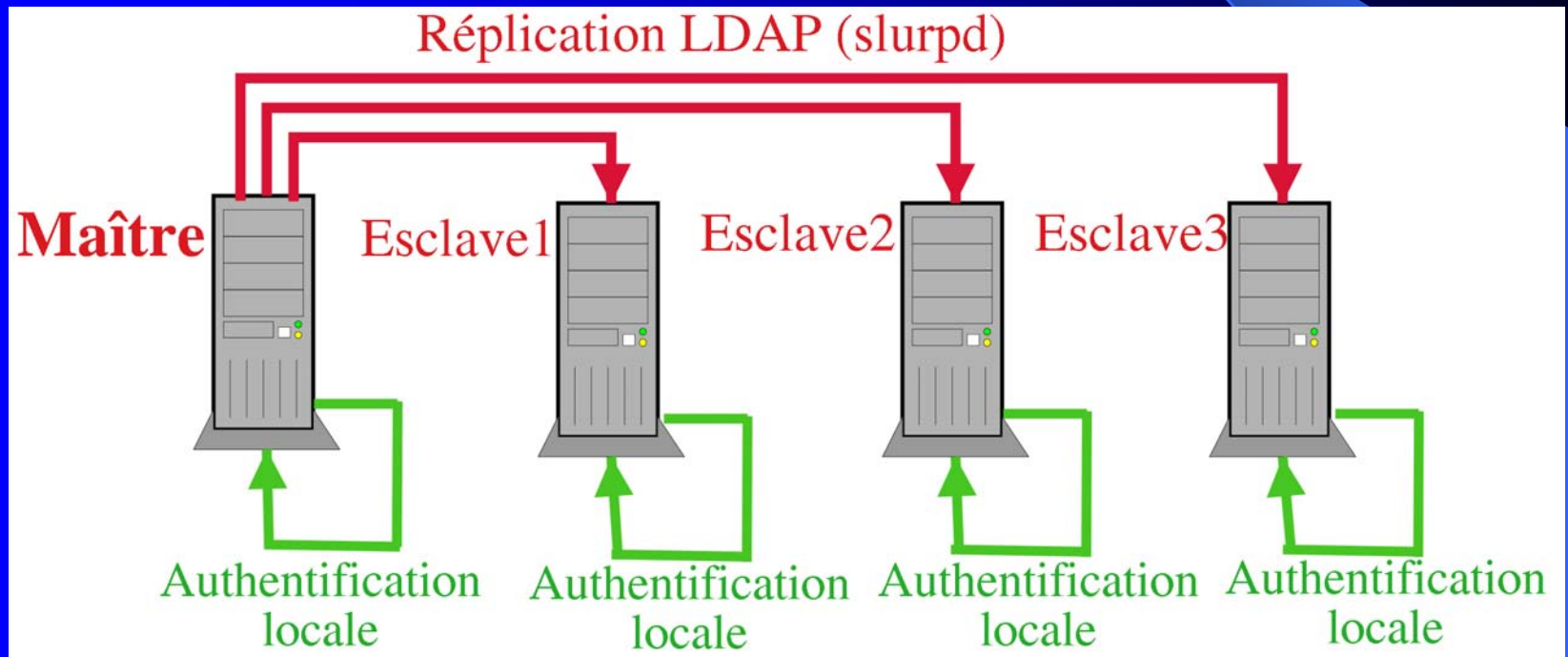
-soumissions des modifications aux slapd esclaves.

Seul le maître peut modifier l'esclave.

LDAP et la réplication :

Intérêts :

- tolérance de pannes,
- répartition de la charge.



La sécurité :

Au niveau communication :
protocole de base : LDAP
protocole sécurisé : LDAP+SSL

Au niveau des privilèges d'accès :
utilisation des ACLs,
utilisation de SASL.

LDAP : base d'authentification



Smb.conf
--with-ldapsam
Samba.schema



Pam-LDAP
Nss-LDAP



Include 2_level_query



Mod_auth_ldap



Authentification Linux avec OpenLDAP :

Utilisation des Pluggable Authentication Modules :
modification du fichier *login*
auth sufficient libpam_ldap.so

bibliothèques ;

libpam-ldap : permet l'authentification,

libnss-ldap : renvoie les infos d'une session,

Paramétrages des fichiers :

nsswitch.conf : pour indiquer l'utilisation LDAP,

/etc/libnss-ldap.conf,

/etc/pam-ldap.conf.

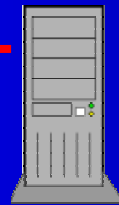
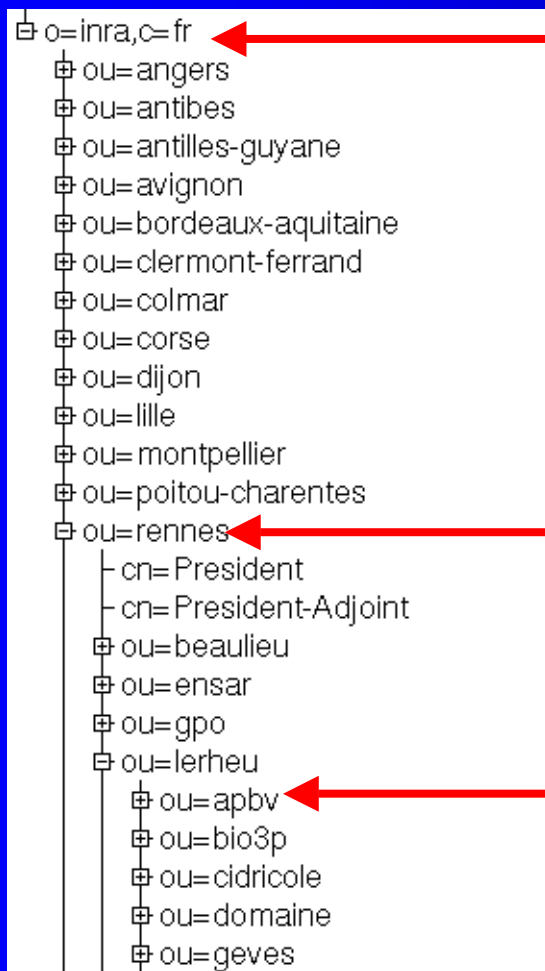
Authentification Linux avec OpenLDAP :

Paramétrages des fichiers libnss-ldap.conf & pam-ldap.conf

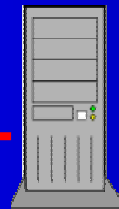
Host	: serveur ldap
SuffixDN	: début de la recherche dans l'annuaire
Scope	: mode de recherche base : niveau du suffixDN, one : + 1 niveau descendant, sub : recherche sur tous les niveaux descendant,
rootDN	: compte de l'administrateur,
rootpw	: mot de passe de l'administrateur.

Authentification Linux avec OpenLDAP :

Importance de la baseDN : Navigation descendante de l'annuaire



Base o=inra,c=fr
Potentiellement tous les utilisateurs



Base ou=rennes,o=inra,c=fr



Base ou=apbv,ou=lerheu,ou=rennes,o=inra,c=fr

Fonctionnement avec SaMBa:

Stable à partir de 2.2.5

Compilation :

`--with-ldapsam`

Installation et paramétrages :

modification du fichiers `smb.conf`

utilisation de `smbpasswd`

Pour Infos :

Samba peut fonctionner avec un serveur LDAP
et être installé sur un serveur qui n'utilise pas LDAP.

Fonctionnement avec SaMBa: Le fichier smb.conf

Global parameters
[global]

parametres de connections LDAP

ldap server = serveur1

ldap port = 389

ldap suffix = "o=inra,c=fr"

ldap admin dn = "cn=admin,o=inra,c=fr"

ldap ssl = yes

Fonctionnement avec SYMPA:

- authentication wwsympa, auth.conf :

ldap

host apbvnet.rennes.inra.fr

suffix ou=users,ou=apbv,ou=lerheu,ou=rennes,o=inra,c=fr

scope one

timeout 10

get_dn_by_uid_filter (&(objectclass=inetorgperson)(uid=[sender]))

email_attribute mail

Fonctionnement avec SYMPA:

-Création de listes dynamiques

Directive include_ldap_2level_query

user_data_source include

include_ldap_2level_query

select2 all

scope2 sub

suffix2 o=inra,c=fr

suffix1 o=inra,c=fr

attrs1 memberuid

user cn=root,o=inra,c=fr

select1 all

filter2 (&(objectclass=posixaccount)(uid=[attrs1]))

timeout1 30

attrs2 mail

scope1 sub

port 389

host apbvnet.rennes.inra.fr

passwd mdp

filter1 (&(objectclass=posixgroup)(cn=colza))

timeout2 30

LDAP et Apache :

- Utilisation d'un des modules :

`mod_auth, auth_ldap ...`

- le fichier `httpd.conf` :

```
<Location /apbv>
```

```
AuthName "Réservé UMR APBV"
```

```
AuthType Basic
```

```
AuthLDAPHosts "apbvnet.rennes.inra.fr"
```

```
AuthLDAPBaseDN "ou=users,ou=apbv,ou=lerheu,ou=rennes,o=inra,c=fr"
```

```
AuthLDAPBindDN "cn=root,o=inra,c=fr"
```

```
AuthLDAPBindPassword vbmrky22
```

```
AuthLDAPSearchScope one
```

```
AuthLDAPUserKey userid
```

```
AuthLDAPPassKey userpassword
```

```
AuthLDAPCryptPasswords on
```

```
AuthLDAPSchemePrefix on
```

```
require valid-user
```

```
</Location>
```

Conclusions:

Le plus important est de bien déterminer son arborescence LDAP pour stocker ses informations.

Points forts :

**la centralisation des comptes utilisateurs,
standardisation des objets,
la facilité de déploiement.**

Point sensible:

utilisation des acs.