

un partage sysvol. Donc les objets LDAP, tel que les GPO, sont indexés dans LDAP et emmagasinés dans le partage sysvol. Comme Samba 3 ne supporte pas le partage sysvol, mais plutôt le partage netlogon (de NT4), l'indexation des objets des GPO dans l'annuaire LDAP ne servent pas vraiment.



NDLR: Les GPO de Microsoft pourraient fonctionner sous un contrôleur de domaine Linux, car la totalité du support des GPO sont intégrées dans le client Windows professionnel. Il ne manque qu'un peu de développement de la part d'un bon samaritain.

Un avantage majeur de l'annuaire LDAP à l'annuaire Active Directory, est lors de l'extension du schéma. L'annuaire d'OpenLDAP est facilement rétractable, alors que celle d'Active Directory ne permet pas la suppression de classes et d'attributs, mais peuvent seulement être désactivé (ce même sur Windows 2003). Le meilleur exemple est l'extension du schéma lors de l'ajout du serveur de messagerie Microsoft Exchange. Il vous est impossible de supprimer les nouveaux objets ajoutés au schéma LDAP.

Schéma de l'annuaire LDAP

Le *schéma de l'annuaire LDAP* est une liste de définitions qui spécifie les types d'informations pouvant être emmagasinés dans l'annuaire LDAP. Vous retrouvez ces schémas dans le répertoire */etc/openldap/schema/* après avoir installé le service LDAP.

Il existe deux types de définition dans le schéma: les *classes* et les *attributs*. Les classes et les attributs sont également appelés objets de schéma ou métadonnées.

Les *attributs* contiennent des éléments de données spécifiques, tel un nom, un numéro de téléphone, un courriel. Dans LDAP, la définition d'un type d'attribut inclus:

- Un nom unique qui identifie le type d'attribut;
- Un identifiant d'objet (OID: *Object Identifier*) qui identifie aussi uniquement l'attribut;
- Une indication qui dit si l'attribut est une valeur simple ou multiple;

NOTES



- Une association à une syntaxe d'attribut et un ensemble de règles correspondantes;
- Un indicateur d'utilisation;
- Une restriction de l'étendu et/ou de la taille des valeurs qui peuvent être emmagasinées dans l'attribut.

Voici un exemple à quoi ressemble un attribut, relié au schéma fournit pour Samba (*samba.schema*).

```
attributetype ( 1.3.6.1.4.1.7165.2.1.25 NAME 'sambaNTPassword'
  DESC 'MD4 hash of the unicode password'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{32} SINGLE-VALUE )
```

Les *classes*, pour leur part, imitent souvent des modèles existants de la vie réelle, comme les personnes, les imprimantes, un périphérique réseau, etc. Ils servent pour regrouper certaines informations et permettent de déterminer:

- Quels types d'attributs *doivent* (*must*) être inclus dans l'entrée;
- Quels types d'attributs *peuvent* (*may*) être inclus dans l'entrée;

Dans LDAP, la définition d'une classe inclus:

- Un nom unique qui identifie le type d'attribut;
- Un OID qui l'identifie également;
- Des attributs obligatoires;
- Des attributs optionnels;
- Un type (structurel, auxiliaire ou abstrait).

Voici un exemple de classe, relié au schéma fournit pour Samba (*samba.schema*).

```
objectclass ( 1.3.6.1.4.1.7165.2.2.4 NAME 'sambaGroupMapping' SUP
top AUXILIARY
  DESC 'Samba Group Mapping'
  MUST ( gidNumber $ sambaSID $ sambaGroupType )
  MAY ( displayName $ description $ sambaSIDList ))
```

NOTES



Planification de mise en oeuvre d'OpenLDAP

Avant de débiter l'installation d'OpenLDAP, nous devons définir à quoi ressemblera notre structure DIT (*Directory Information Tree*). La structure DIT correspond à l'arborescence de votre domaine et doit généralement ressembler à l'organisation.

Vous devez analyser la structure et le fonctionnement de votre entreprise et concevoir en conséquence, la structure de domaine, l'espace de nom du domaine, la structure d'unité organisation et la structure de sites si nécessaires.

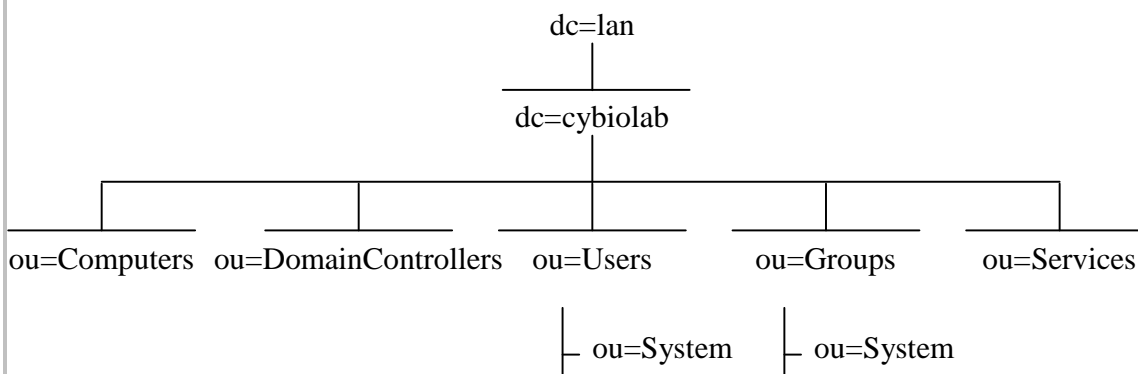


NOTE: Nous n'aborderons pas le concept de site dans cette version de manuel. L'intégration de site nécessite l'ajout de nouveaux paramètres dans Samba et une réplification de l'annuaire LDAP différente que celle proposée dans le manuel.

Dans notre cas nous désirons un annuaire LDAP qui sera accessible que de l'intérieur de l'entreprise et n'aura donc aucun accès par Internet. Par contre nous allons garder une compatibilité en utilisant un espace de nom plat (*flat namespace*).

Faisons une relation avec les services précédemment installés. Le service Samba a défini que notre nom de domaine serait cybiolab. Le service BIND, lui, fait la résolution DNS, pour cybiolab.lan. Notre structure DIT débutera donc par *dc=cybiolab,dc=lan*.

Voici donc notre structure DIT qui va nous servir de base pour l'élaboration de l'arborescence pour notre domaine cybiolab.lan.



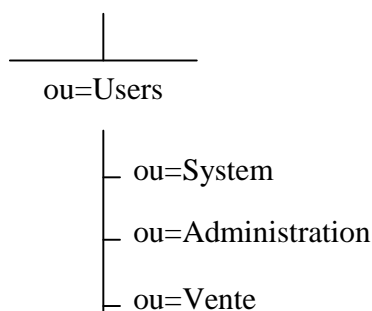
Cette structure DIT est fortement similaire à celle utilisé par Microsoft (Windows) ou par Apple (MacOS X).

NOTES



L'unité organisationnelle *Users* va nous servir pour y enregistrer les utilisateurs du domaine. Il servira aussi pour l'authentification des utilisateurs sur le domaine. La sous-unité organisationnelle *System* va vous permettre d'y enregistrer vos comptes de domaine système afin de ne pas les mélanger avec les comptes communs.

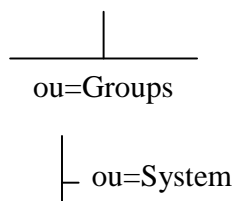
Il vous suffit d'y ajouter votre propre structure d'unité d'organisation sous *Users* pour classer vos utilisateurs. Nous vous conseillons d'utiliser vos noms de département pour la création des unités d'organisation. Par exemple:



L'unité organisationnelle *Computers* va nous servir pour y enregistrer les ordinateurs du domaine. Il servira aussi pour l'authentification des ordinateurs clients sur le domaine par le service Samba.

L'unité organisationnelle *DomainControllers* est en fait une simple fantaisie et va nous servir pour y enregistrer les contrôleurs de domaine. Il servira à l'authentification des contrôleurs de domaine secondaires sur le domaine.

L'unité organisationnelle *Groups* va nous servir pour y enregistrer des groupes du domaine. Il servira pour les permissions sur les fichiers et autres ressources sur le réseau. La sous-unité organisationnelle *System* va vous permettre d'y enregistrer vos groupes systèmes afin de ne pas les mélanger avec les comptes communs



Nous allons étendre, plus tard, notre schéma LDAP pour y ajouter des fonctionnalités intéressantes tel le sudo.

NOTES



