Programmation en PHP
Cyril Beaussier

Utilisation de LDAP

Version 1.0 – Juin 2005

COPYRIGHT ET DROIT DE REPRODUCTION

Si vous souhaitez des améliorations, je suis évidemment ouvert à toute suggestion. Il en est de même si vous constatez une erreur (nul n'est parfait). Pour cela, il suffit de m'écrire avec pour sujet « *Programmation en PHP / Utilisation de LDAP* » dans la rubrique « *Contact* » de mon site principal :

www.beaussier.com

En revanche, je n'assure aucune aide, ni support sur des questions de programmation ou de compréhension de ce manuel. Je vous invite à vous reporter sur les excellents forums de Developpez.com (section *PHP*) où je traîne régulièrement.

Je ne suis lié avec aucun éditeur ou constructeur informatique.

Ce support a été réalisé avec la suite bureautique libre *Open Office* 1.1 (disponible gratuitement sur http://fr.openoffice.org) qui permet d'exporter nativement en PDF.

Avertissement complémentaire :

Les éléments (données ou formulaires) éventuellement inclus dans ce support vous sont fournis à titre d'exemple uniquement. Leur utilisation peut avoir, dans certains cas, des conséquences matériels et juridiques importantes qui peuvent varier selon le sujet dont ils traitent. Il est recommandé d'être assisté par une personne compétente en informatique ou de consulter un conseiller juridique ou financier avant de les utiliser ou de les adapter à votre activité.

Sommaire

1. INTRODUCTION.....5

2. QU'EST CE QUE LDAP ?.....6

3. POURQUOI UTILISER LDAP ?.....9

4. INSTALLATION DU SERVEUR LDAP..... 10

5. UTILISATION DE LDAP.....13

6. PREMIÈRE CONNEXION..... 14

7. AJOUT DANS L'ANNUAIRE.....16

7.1. Ajout d'un pays..... 17

7.2. Ajout d'une organisation.....18

7.3. Ajout d'une unité..... 19

7.4. Ajout d'une personne.....20

8. LIRE DANS L'ANNUAIRE.....21

9. CONCLUSION..... 23

1. Introduction

Ce manuel est ici pour vous apprendre à **utiliser les fonctions LDAP depuis PHP** et non pas à débuter en PHP. Je pars donc du principe que vous n'êtes pas un néophyte et que vous connaissez déjà les bases de la programmation dans ce langage.

Remarque :

Bien que PHP 5 soit la dernière version disponible, je n'aborde dans ce manuel que la syntaxe et les possibilités de **PHP 4**. J'ai seulement annoté par endroit certaines évolutions qui me paraissaient importantes.

Pour la rédaction des exemples de code, j'utilise donc au minimum PHP dans sa version **4.1.0** (qui est d'ailleurs déjà ancienne). Ceci est notamment valable pour la syntaxe des fonctions et surtout des variables **superglobales**. Si vous développez avec une version antérieure, je vous conseille de vous reporter sur la documentation officielle pour la correspondance des fonctions.

Pour la programmation, je me sers du célèbre **EasyPHP** dans sa version 1.7 (disponible gratuitement sur www.easyphp.org). Je ne détaille pas la procédure d'installation et vous renvoie sur leur site pour ces détails.

Pour le serveur LDAP, j'utilise **OpenLDAP** de Lucas Bergman. C'est un logiciel à code ouvert (*open source*) disponible sur plateforme Linux et Windows.

2. Qu'est ce que LDAP ?

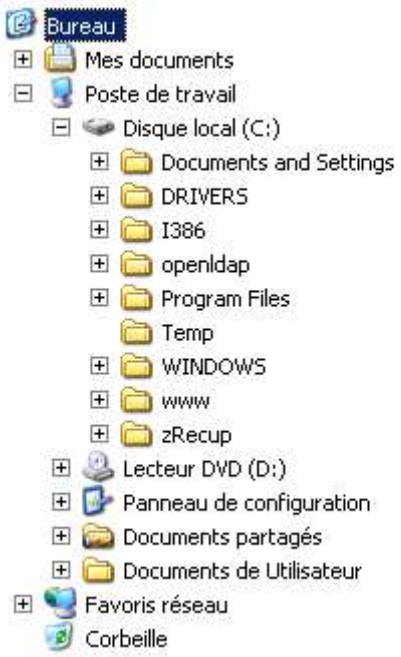
Si bien sûr vous n'avez jamais entendu parler de LDAP (ou alors de loin), c'est une question qui peut donc se poser.

LDAP est un acronyme anglais pour *Lightweight Directory Access Protocol* qui peut se traduire par *Protocole d'Accès d'Annuaire Allégé*. LDAP est donc un protocole tout comme HTTP ou FTP. C'est à dire un ensemble de règles qui permet d'établir un échange de données entre deux ordinateurs.

LDAP est en fait une base de données regroupant des identités d'utilisateurs. Cela part des nom et prénom, du login et bien sûr du mot de passe. Vous pouvez également y ajouter tout autre type d'information que vous jugez utile d'y stocker : adresse, courriel, téléphone, etc.

Toutes ces données sont dans la base et hiérarchisées sous la forme d'une arborescence un peu à la manière d'un disque où vous retrouvez des dossiers, sous-dossiers et fichiers.

A droite, l'arborescence d'un ordinateur sous Windows :



Pour identifier un fichier sur votre ordinateur, vous utilisez un chemin. Par exemple :

```
/progra~1/easyph~1/www/index.php
```

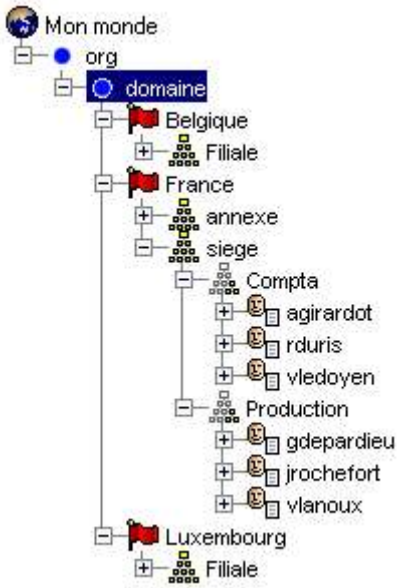
Remarque :

La notation des fichiers est déclarée en 8.3 (MS-DOS) pour éviter tout problème de gestion d'espace.

La barre oblique indique une séparation dans la référence, et la ligne doit être lue de la gauche vers la droite. Nous allons voir qu'avec LDAP, c'est un peu différent.

Le concept est similaire et on parle alors de contexte LDAP. Dans de nombreux annuaires, vous retrouverez à peu près la même arborescence.

Voici un exemple de contexte LDAP :



Le niveau le plus haut n'est plus votre « Bureau » mais le « Monde » dans lequel se trouve votre annuaire. Nous aurons ensuite un premier niveau de « Pays ». Un deuxième niveau rassemblant les structures : entreprise, bâtiment ou organisation. Nous aurons ensuite les départements, emplacements ou secteurs et pour terminer, les personnes, utilisateurs ou membres.

Pour identifier un utilisateur dans un annuaire, on utilise une chaîne appelée **DN** pour « *Distinguished Name* » et qui se traduit par « *Nom distingué* ».

Prenons par exemple, l'utilisateur **vledoyen**, son DN sera défini comme suit :

```
cn=vledoyen,ou=Compta,o=siege,c=France,dc=domaine,dc=org
```

C'est une virgule qui marque la séparation de chaque niveau. Chaque niveau est précédé d'une abréviation correspondant au nom de l'entité. La séquence est lue cette fois de droite à gauche. Dans l'exemple ci-dessus, il faut donc lire :

```
directoryContext=org
directoryContext=domaine
country=France
organization=siege
organizationalUnit=Compta
commonName=vledoyen
```

Remarque :

Il n'y a pas vraiment de règle en matière d'organisation LDAP. Vous orchestrez donc votre annuaire de manière à ce qu'il soit le plus pratique pour vous.

Suivant la complexité de votre structure, vous aurez plus ou moins de niveaux. Vous êtes libre d'ajouter ou de supprimer certains niveaux ou objets. Ainsi, si votre entreprise n'est pas internationale, vous pourrez supprimer le niveau « Pays » et ajouter un niveau « Région ».

3. Pourquoi utiliser LDAP ?

La gestion des identités est primordiale sur un réseau. Il faut bien sûr authentifier les utilisateurs afin de savoir s'ils peuvent accéder ou non aux ressources (fichiers, imprimantes, applications ou base de données).

Lorsque vous développez une application qui a une implication dans l'entreprise, vous allez très vite avoir besoin d'identifier les utilisateurs.

Vous pouvez alors programmer votre propre système d'identification (utilisateur / mot de passe). Mais cela devient vite contraignant car vous devez gérer vous-même la création de tous ces comptes.

Le mieux est donc d'utiliser le système LDAP. Un annuaire qui rassemble déjà toute l'organisation de votre entreprise et tous ses comptes utilisateur. Il ne vous reste plus qu'à « piocher » dans cette base de données les informations qui vous sont nécessaires.

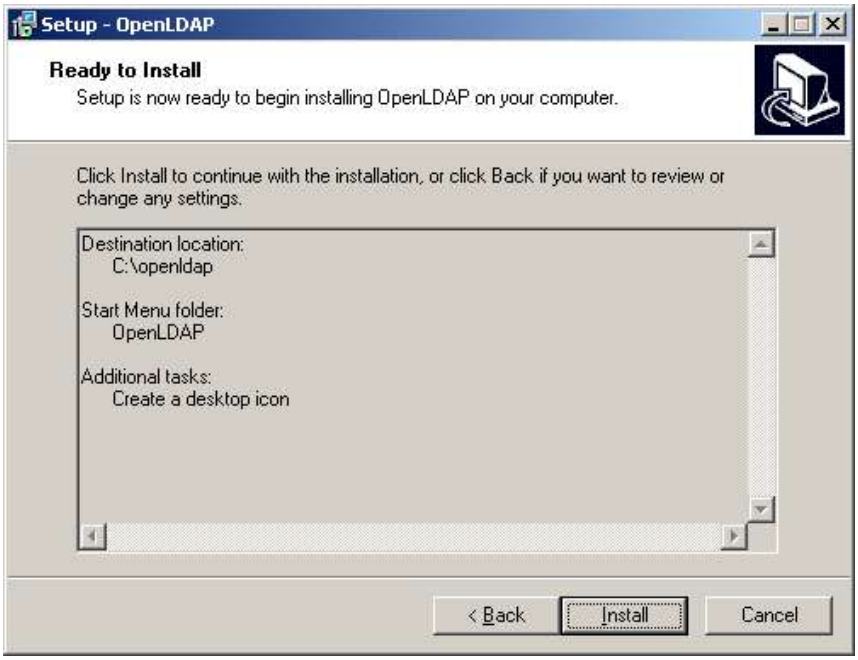
4. Installation du serveur LDAP

Comme je l'ai précisé dans l'introduction, nous allons nous servir d'un serveur très répandu sur plateforme Unix et bien sûr Linux : **OpenLDAP**. Cet annuaire à code ouvert est également disponible sous Windows.

Grâce à Lucas Bergman, vous pouvez donc installer un binaire Win32 de **OpenLDAP** sur votre ordinateur en le téléchargeant à l'adresse :

`http://download.bergmans.us/openldap`

Une fois fait, lancez l'installation, acceptez la licence et modifiez éventuellement le répertoire par défaut : `[c:/openldap]`. Validez tous les autres écrans pour la création éventuelle des raccourcis.



Nous allons ensuite éditer le fichier **slapd.conf** qui contient la configuration du serveur afin de paramétrer notre annuaire avant de le lancer. Dans l'extrait ci-dessous, j'ai mis en bleu les lignes que vous devez modifier :

```
#######################################################################
# BDB database definitions
#######################################################################

database    bdb
suffix            "dc=domaine,dc=org"
rootdn            "cn=Manager,dc=domaine,dc=org"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw            secret
```

Il s'agit de choisir un **suffixe**. C'est en fait la racine de votre serveur. Toutes les entrées que vous ajouterez par la suite dans l'annuaire, seront attachées à ce suffixe. Pour notre exemple, nous aurons le suffixe `[dc=domaine,dc=org]`.

Il faut ensuite modifier l'entrée de l'administrateur de l'annuaire. Il s'agit de la ligne `rootdn` à laquelle nous mettrons le suffixe correct. Par défaut, il a pour nom « Manager » mais vous pouvez changer son nom.

Remarque :

La ligne `rootpw` contient le **mot de passe** de l'administrateur. Par défaut, celui-ci vaut « secret » et se trouve en clair. Il est fortement recommandé en production de le changer et de passer en authentification forte avec un cryptage MD5.

L'exécutable **slapd.exe** correspond à votre serveur **OpenLDAP**. Vous pouvez le lancer en tant que programme autonome ou en tant que service. Personnellement en phase de développement, je préfère la première solution.

Créez un raccourci sur celui-ci afin de faciliter son lancement.

Double cliquez sur le raccourci depuis votre bureau. Une fenêtre console MS-DOS s'ouvre sans aucun message. C'est votre serveur **OpenLDAP** qui est désormais lancé.

Remarque :

Bien sûr, vous ne devez pas fermer cette fenêtre pendant toute la durée de vos tests. Pour ne pas être gêné, vous pouvez la réduire en barre de tâches.

Il nous reste maintenant à créer la racine « Domaine » de notre annuaire. Pour cela, nous allons créer un fichier contenant notre première entrée. Tapez le texte ci-dessous :

```
dn: dc=domaine,dc=org
objectclass: top
objectclass: dcObject
objectclass: organization
o: Domaine
dc: domaine
```

Sauvegardez ce fichier texte sous le nom **init.txt** dans le répertoire de votre annuaire : `[c:/openldap]`.

Ouvrez une fenêtre console MS-DOS et tapez les commandes suivantes (en bleu) :

```
C:\> cd \openldap
C:\openldap> slapadd -f slapd.conf -l init.txt
```

Normalement, rien ne s'affiche et le système vous rend la main. Vous pouvez fermer la fenêtre.

5. Utilisation de LDAP

Tout est prêt maintenant pour utiliser notre annuaire. Avant de commencer, il convient de lister les fonctions qui vont nous servir pour utiliser LDAP.

Remarque :

Attention, nous n'allons pas utiliser toutes les fonctions dont dispose PHP et je vous invite à vous reporter sur la documentation officielle.

Fonction	**Définition**
`ldap_add`	Ajoute une entrée dans LDAP
`ldap_bind`	S'attache au serveur LDAP
`ldap_close`	Termine la connexion du serveur LDAP
`ldap_connect`	Se connecte à un serveur LDAP
`ldap_count_entries`	Compte le nombre d'entrées après une recherche
`ldap_get_entries`	Lit toutes les entrées du résultat
`ldap_search`	Recherche dans LDAP
`ldap_set_option`	Modifie la valeur d'une option

6. Première connexion

Voici un premier script pour vérifier que la connexion au serveur **OpenLDAP** et que l'attachement en tant qu'utilisateur anonyme fonctionne bien.

Si la fonction **ldap_connect** ouvre une connexion au serveur LDAP, c'est **ldap_bind** qui permet l'authentification en passant en paramètre un DN et un mot de passe. Dans le script, nous utilisons **ldap_bind** sans DN, ce qui implique une connexion anonyme.

```php
<?php
echo "<h3>Test LDAP n° 1</h3>";
echo "Connexion ...<br />";
$ds = ldap_connect ("localhost");
echo "Le résultat est ".$ds."<br />";

if ($ds)
{
    echo "Attachement...";
    $r = ldap_bind ($ds);
    echo "Le résultat est ".$r."<br />";

    echo "Fermeture de la connexion";
    ldap_close ($ds);

}
else
{
    echo "Impossible de se connecter au serveur LDAP";
}
?>
```

Si vous testez ce script, il ne fonctionne pas. Votre navigateur va afficher :

Test LDAP n° 1

Connexion ...
Le résultat est Resource id #2
Attachement...
Warning: ldap_bind(): Unable to bind to server: Protocol error in
c:\program files\easyphp1-7\www\ldap\ldap_01.php on line **10**
Le résultat est
Fermeture de la connexion

Le message d'erreur retourné par PHP est très clair : il est impossible de s'attacher au serveur car il y a une erreur de protocole.

Notre serveur **OpenLDAP** est en effet en version de protocole 3 et par défaut PHP envoie ses ordres en version 2. Nous allons donc modifier notre script en paramétrant le protocole avec **ldap_set_option**.

```
<?php
echo "<h3>Test LDAP n° 1</h3>";
echo "Connexion ...<br />";
$ds = ldap_connect ("localhost");
echo "Le résultat est ".$ds."<br />";

if ($ds)
{
    ldap_set_option ($ds, LDAP_OPT_PROTOCOL_VERSION, 3);

    echo "Attachement...";
    ...
```

Si vous retentez maintenant, vous constatez que l'attachement anonyme fonctionne.

Test LDAP n° 1

Connexion ...
Le résultat est Resource id #2
Attachement... Le résultat est 1
Fermeture de la connexion

7. Ajout dans l'annuaire

Nous allons maintenant enrichir notre annuaire en ajoutant des entrées à l'intérieur. Nous allons ainsi créer toute l'arborescence de notre annuaire.

Pour cela, nous devons **obligatoirement** nous identifier en tant qu'administrateur ou super utilisateur. Nous allons donc reprendre la chaîne DN avec notre **manager** et le mot de passe déclaré dans le fichier **slapd.conf**.

```
<?php

$dn = "cn=Manager,dc=domaine,dc=org";
$pwd = "secret";

echo "<h3>Test d'ajout dans LDAP</h3>";
$ds = ldap_connect ("localhost");

if ($ds)
{
    ldap_set_option ($ds, LDAP_OPT_PROTOCOL_VERSION, 3);

    // Attachement administrateur
    ldap_bind ($ds, $dn, $pwd);

    // Vient ensuite le code pour ajouter
    ...
```

Une fois authentifié, nous pouvons ajouter notre entrée qui est appelé RDN (pour *Relative Distinguished Name*). Il s'agit d'un DN mais qui doit être relatif à l'arborescence de votre annuaire.

Suivant le type d'objet que vous voulez ajouter, vous allez passer certains attributs de base.

7.1. Ajout d'un pays

Nous allons d'abord créer le premier niveau avec le pays. Le niveau pays (*country* en anglais) se déclare avec les attributs suivants :

Attribut	Valeur
c	Nom du pays
objectClass	country
objectClass	top

Cela nous donne pour notre script, le code ci-dessous :

```
    // On s'est d'abord authentifier

    // Préparation des données
    $info ["c"] = "France";
    $info ["objectClass"][0] = "country";
    $info ["objectClass"][1] = "top";
    $rdn = "c=".$info ["c"].",dc=domaine,dc=org";

    // Ajout
    $r = ldap_add ($ds, $rdn, $info);
    if ( $r ) echo $rdn." a été ajouté !";
}
ldap_close ($ds);
?>
```

Si vous testez ce script, votre navigateur va afficher :

Test d'ajout dans LDAP

c=France,dc=domaine,dc=org a été ajouté !

Ajoutez les entrées pour **Belgique** et **Luxembourg** pour vous conformer à notre arborescence d'annuaire exposée au chapitre 2. Qu'est ce que LDAP ?

7.2. Ajout d'une organisation

L'organisation est le deuxième niveau de notre annuaire. Celle-ci se déclare avec les attributs suivants :

Attribut	Valeur
o	Nom de l'organisation
objectClass	organization
objectClass	top

Cela nous donne pour notre script, le code ci-dessous :

```
    // On s'est d'abord authentifier

    // Préparation des données
    $info ["o"] = "Siege";
    $info ["objectClass"][0] = "organization";
    $info ["objectClass"][1] = "top";
    $rdn = "o=".$info ["o"].",c=France,dc=domaine,dc=org";

    // Ajout
    $r = ldap_add ($ds, $rdn, $info);
    if ( $r ) echo $rdn." a été ajouté !";
}
ldap_close ($ds);
?>
```

Si vous testez ce script, votre navigateur va afficher :

Test d'ajout dans LDAP

o=Siege,c=France,dc=domaine,dc=org a été ajouté !

Vous pouvez continuer en créant les autres organisations : **Annexe** et **Filiale** dans chaque pays.

7.3. Ajout d'une unité

L'unité organisationnelle est le troisième niveau de notre annuaire. Celle-ci se déclare avec les attributs suivants :

Attribut	Valeur
ou	Nom de l'unité
objectClass	organizationalUnit
objectClass	top

Cela nous donne pour notre script, le code ci-dessous :

```
    // On s'est d'abord authentifier

    // Préparation des données
    $info ["ou"] = "Production";
    $info ["objectClass"][0] = "organizationalUnit";
    $info ["objectClass"][1] = "top";
    $rdn = "ou=".$info ["ou"].",o=Siege,c=France,dc=domaine,dc=org";

    // Ajout
    $r = ldap_add ($ds, $rdn, $info);
    if ( $r ) echo $rdn." a été ajouté !";
}
ldap_close ($ds);
?>
```

Si vous testez ce script, votre navigateur va afficher :

Test d'ajout dans LDAP

ou=Production,o=Siege,c=France,dc=domaine,dc=org a été ajouté !

Vous pouvez continuer en créant les autres unités organisationnelles : **Marketing** ou **Comptabilité**.

7.4. Ajout d'une personne

La personne est le dernier niveau de notre annuaire. Celle-ci se déclare avec les attributs suivants :

Attribut	Valeur
cn	Nom commun de la personne
sn	Nom unique de la personne
userPassword	Mot de passe
objectClass	person
objectClass	top

Cela nous donne pour notre script, le code ci-dessous :

```
    // Préparation des données
    $info ["cn"] = "cbeaussier";
    $info ["sn"] = "Beaussier Cyril";
    $info ["userPassword"] = "chut";
    $info ["objectClass"][0] = "person";
    $info ["objectClass"][1] = "top";
    $rdn = "cn=".$info ["cn"].
           ",ou=Production,o=Siege,c=France,dc=domaine,dc=org";

    // Ajout
    $r = ldap_add ($ds, $rdn, $info);
    if ( $r ) echo $rdn." a été ajouté !";
}
ldap_close ($ds);
?>
```

Si vous testez ce script, votre navigateur va afficher :

Test LDAP n° 2

cn=cbeaussier,ou=Production,o=Siege,c=France,dc=domaine,dc=org a été ajouté !

Pour que l'annuaire ait quelques utilisateurs, retentez l'opération avec d'autres entrées de votre choix.

Remarque :

Pour des questions de confidentialité, il est préférable de crypter le mot de passe de l'utilisateur avec la fonction **md5**.

8. Lire dans l'annuaire

Voilà ! Votre annuaire contient maintenant un certain nombre d'informations. Il s'agit maintenant de pouvoir les extraire ou les filtrer suivant des critères de recherche.

Remarque :

Pour les opérations de recherche qui ne sont que de la lecture, vous pouvez vous connecter en tant qu'anonyme.

```php
<?php

echo "<h3>Recherche dans LDAP</h3>";
$ds = ldap_connect ("localhost");

if ($ds)
{
    ldap_set_option ($ds, LDAP_OPT_PROTOCOL_VERSION, 3);

    // Attachement anonyme
    ldap_bind ($ds);

    // Combien ais-je de personne dans mon annuaire ?
    $sr = ldap_search ($ds, "dc=domaine,dc=org", "sn=*");
    echo "Le résultat de la recherche est ".$sr."<br />";

    $nb = ldap_count_entries ($ds, $sr);
    echo "Nombre d'entrées retournées : ".$nb;
}
ldap_close ($ds);
?>
```

Dans le script ci-dessus, on cherche à savoir combien de personnes se trouve référencées dans l'annuaire. Pour cela, on spécifie dans la chaîne de recherche, l'attribut **sn** avec le caractère joker * (l'étoile).

Recherche dans LDAP

Le résultat de la recherche est Resource id #3
Nombre d'entrées retournées : 16

Dressons maintenant une liste partielle des utilisateurs de notre annuaire avec le script suivant :

```php
<?php

echo "<h3>Recherche dans LDAP</h3>";
$ds = ldap_connect ("localhost");

if ($ds)
{
    ldap_set_option ($ds, LDAP_OPT_PROTOCOL_VERSION, 3);

    // Attachement anonyme
    ldap_bind ($ds);

    // Liste des personnes commençant par D
    $sr = ldap_search ($ds, "dc=domaine,dc=org", "sn=D*");
    $info = ldap_get_entries ($ds, $sr);
    echo "Nombre de personnes trouvées : ".$info ["count"]."<p>";

    for ($i=0; $i < $info ["count"]; $i++)
    {
        echo "dn : ". $info[$i]["dn"] ."<br>";
        echo "cn : ". $info[$i]["cn"][0] ."<br>";
        echo "sn : ". $info[$i]["sn"][0] ."<p>";
    }
}
ldap_close ($ds);
?>
```

Ce qui va nous donner :

Recherche dans LDAP

Nombre de personnes trouvées : 2

dn : cn=adelon,ou=Compta,o=siege,c=France,dc=domaine,dc=org
cn : adelon
sn : Delon Alain

dn : cn=gdepardieu,ou=Production,o=Siege,c=France,dc=domaine,dc=org
cn : gdepardieu
sn : Depardieu Gérard

9. Conclusion

Et voilà ! Avec ce support, nous venons de couvrir les bases pour l'utilisation d'un annuaire LDAP avec PHP.

Pour plus d'information sur les annuaires LDAP, voici deux autres manuels qui sont disponibles sur le site Developpez.com :

http://mirtain.developpez.com/tutoriel/ldap/
http://mparienti.developpez.com/cours/openldap/

Je vous invite également sur mon site principal où vous retrouverez d'autres supports pour aller plus loin en PHP. Reportez-vous pour cela à l'adresse suivante :

www.beaussier.com/?pg=doc