

## Création des utilisateurs

Il existe deux principaux types de compte utilisateur: les **comptes utilisateurs locaux** et les **comptes utilisateurs du domaine**.

Ce manuel vous montre comment créer des utilisateurs sur les contrôleurs de domaine Linux. Pour notre projet, nous utiliserons principalement que des comptes utilisateurs du domaine.

### Utilisateurs Locaux

Les utilisateurs locaux peuvent être utilisés pour offrir une authentification directement sur le contrôleur de domaine. Cela peut être intéressant dans le cas où votre annuaire LDAP est inopérant. Avoir un utilisateur local, faisant parti du groupe *wheel* est toujours un atout majeur en cas de panne. Cependant pour les comptes des utilisateurs standards, nous vous conseillons d'utiliser le plus possible les comptes utilisateurs du domaine.

Traditionnellement les entrées des utilisateurs sont emmagasinées dans le fichier *passwd* situé dans le répertoire */etc*. Aussi, les mots de passe sont emmagasinés dans le fichier *shadow*, toujours dans le répertoire */etc*. Ces fichiers sont de simple fichier texte comprenant une série d'entrées. Ces entrées se composent de différents champs séparés par des ":" :

```
nom_utilisateur:mot_de_passe:numéro_utilisateur:numéro_de_groupe_principal :commentaire:répertoire_personnel:interpréteur_de_commandes
```

Pour éditer manuellement le fichier utilisateur (ce que nous ne vous recommandons pas, sauf si vous savez ce que vous faites), utiliser l'une des commandes suivantes,

```
vim /etc/passwd  
vim /etc/shadow
```

ou encore sous Gentoo.

```
vipw
```

Pour savoir si un utilisateur est reconnu sur un ordinateur, saisissez la commande suivante dans une console.

```
id <nom_de_l'utilisateur>
```

NOTES







## Utilisateurs du Domaine

Un compte utilisateur du domaine permet à un utilisateur de s'authentifier sur le domaine, peut importe le poste sur lequel il ouvre une session. Ce type de compte est valable tant pour les postes Windows que sous Linux.

Les entrées des utilisateurs sont emmagasinées dans l'annuaire LDAP de votre domaine. Cette centralisation a comme avantage de faciliter la gestion des utilisateurs.

Tout comme avec les utilisateurs locaux, pour savoir si un utilisateur existe, il suffit simplement de saisir la commande suivante dans une console.

```
id <nom_de_l'utilisateur>
```

Aussi pour connaître tous les utilisateurs existant (et utilisable par l'ordinateur) tant les utilisateurs locaux, que les utilisateurs du domaine, saisissez la commande en console.

### getent passwd

Remarquer que certain utilisateur peuvent apparaître en double, tel que l'utilisateur root. C'est un exemple de chevauchement de nom.

### Création d'un utilisateur du domaine.

1. Ouvrez l'outil web phpLDAPAdmin.
2. Dans le volet de gauche, cliquer sur le "plus" de l'unité organisation "Users".
3. Puis cliquer sur "Create new entry here".
4. Choisissez "Domain User".
5. Vous devez maintenant entrer les valeurs aux attributs pour la création de votre utilisateur.

Sur la première page, vous retrouverez les renseignements de création de l'utilisateur.

Le champ **Container DN**, qui devrait pointer sur l'unité d'organisation `ou=Users` ou un de ses sous-unités dans votre domaine.

### NOTES



Les champs **First name** et **Last name** sont généralement à titre indicatif, mais dans ce modèle de création, il servira à compléter automatiquement d'autres champs (CN, SN, homeDirectory, displayName, etc.) dans l'assistant de création d'utilisateur.

Donc prenez soin de bien remplir ces champs en respectant les consignes suivantes:

- N'insérer aucun espacement dans ces champs,
- Utilisez des caractères qui respectent les normes pour le nommage d'une entrée LDAP.

Les champs **Common Name** et **User logon name** restent idéalement identiques. Cela permet de faciliter la gestion et la recherche plus tard dans votre annuaire LDAP.

Encore ici, assurez-vous que ces champs ne contiennent pas d'espacement, et respecte les normes LDAP pour le nommage d'une entrée CN.

Le champ **UID number** permet une identification unique de l'utilisateur sur un poste ou serveur Linux. Assurez-vous que,

- le nombre que vous inscrivez ne chevauche pas un autre UID dans l'annuaire LDAP incluant ceux des ordinateurs,
- Le nombre n'est doit pas être inférieur au UID 500 (inclusivement). Ces UID sont réservés exclusivement pour les comptes systèmes,
- Le nombre du UID ne doit pas dépasser le nombre 65535 (inclusivement).

Le champ **Samba SID** pour sa part, permet une identification unique de l'utilisateur sur un poste ou un serveur Windows, ainsi que sur le domaine Linux.

Le SID typique se décompose ainsi *S-1-5-21-{Domaine}-{ID}* où

S-1-5-21-      SID connus (wellknown) - NT non-unique.

{Domaine}-    Numéro unique identifiant le domaine. Ce numéro est emmagasiné dans le fichier *secret.tdb*.

{ID}            Numéro d'identifiant unique pour un utilisateur.

## NOTES







- Pager
- Telephone (Home)

Tous les champs de cette page sont optionnels.



**Attention:** Le champ Courriel est parfois utiliser par certaines applications Linux comme nom de login. Par exemple bugzilla de Mozilla.

NOTES



### Suppression d'un utilisateur du domaine.

La suppression d'un utilisateur du domaine est une opération irrévocable, qui s'effectue en trois opérations.

1. Allez dans le contexte de l'utilisateur pour sélectionner l'utilisateur que vous désirez supprimer.
2. Dans le menu du haut de la fenêtre de droite, cliquer sur **Delete this entry**.
3. Une confirmation vous sera alors demandée. Pesez sur **Delete**.

### Modification d'un utilisateur du domaine.

L'outil phpLDAPAdmin permet de rapidement faire des modifications sur un objet LDAP, soit renommer un utilisateur, modifier une entrée dans un champ ou encore ajouter un nouvel attribut à un utilisateur.

### Renommer le nom d'un utilisateur du domaine.

Le renommage de l'objet utilisateur est seulement pour le nom qui sert pour l'authentification sur le domaine ou sur un partage Samba.

1. Pour renommer un objet, sélectionner l'objet dans le contexte puis dans le menu du haut choisir **Rename**.

2. Changer le nom en prenant soin de laisser le *uid=* devant le nouveau nom de l'utilisateur.

### Modifier/Supprimer un champ d'un utilisateur du domaine.

1. Changer le ou les champs que vous désirez changer la valeur, puis peser sur le bouton **Save Changes**.
2. Validez ensuite les changements effectués.

### Ajouter un nouvel attribut à un utilisateur du domaine.

1. Allez dans le contexte de l'utilisateur pour sélectionner l'utilisateur que vous désirez ajouter un nouvel attribut.
2. Dans le menu du haut de la fenêtre de droite, cliquez sur **Add new attribute**.
3. Choisir l'attribut désiré dans le menu déroulant de gauche et inscrivez la valeur dans la zone de texte de droite. Puis pesez sur le bouton **Add**.

### Déplacement d'un utilisateur du domaine.

1. Allez dans le contexte de l'utilisateur pour sélectionner l'utilisateur que vous désirez déplacer.
2. Dans le menu du haut de la fenêtre de droite, cliquez sur **Copy or move this entry**.
3. Choisissez le chemin de destination, en prenant bien soin de laisser l'identifiant de l'utilisateur (CN ou UID).
4. Cocher la case **Delete after copy (move)**. Puis cliquer sur **Copy**.

### Exportation d'un utilisateur du domaine.

Le LDIF (*LDAP Data Interchange Format*) est un format de fichier pour l'*importation* et l'*exportation* d'objet au sein d'annuaire LDAP. Ce format est supporté tant par Active Directory de Microsoft, de Domino Directory de IBM que de NDS de Novell. En somme, c'est un standard pour la norme X509.

NOTES



Voici un exemple de fichier LDIF, d'un utilisateur exporté du domaine Cybiolab.lan

#### Exemple de fichier LDIF

```
version: 1

# Exportation LDIF pour : uid=drobbins,ou=Users,dc=cybiolab,dc=lan
# Généré par phpLDAPadmin ( http://phpldapadmin.sourceforge.net/ ) pour
November 28, 2006 12:45 am
# Serveur: Cybiolab.lan (192.168.0.2)
# Portée de la recherche: base
# Filtre de recherche: (objectClass=*)
# Entrées totales: 1


dn: uid=drobbins,ou=Users,dc=cybiolab,dc=lan
cn: Daniel
displayName: Daniel Robbins
homeDirectory: /home/drobbins
loginShell: /bin/bash
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
sambaAcctFlags: [U      ]
sambaHomeDrive: Y:
sambaHomePath: \\serveurpdc.cybiolab.lan\profiles\drobbins
sambaLogonScript: Commun.vbs
sambaPrimaryGroupSID: S-1-5-21-1234567890-1234567890-1223456789-513
sambaProfilePath: \\serveurpdc.cybiolab.lan\profiles\drobbins
uid: drobbins
description: Utilisateur du Domaine
sambaSID: S-1-5-21-1234567890-1234567890-1223456789- 3000
gidNumber: 100
uidNumber: 1000
sambaLMPassword: 29D384F389B2C91DC5D3B53DC1AA2319
sambaNTPassword: BD29F5A1766BEF5E3784166F3A8413BF
userPassword: {SSHA}qdOCRdMK1N3s/tky5bJ5WTN3x2Km0a5B
```

1. Allez dans le contexte de l'utilisateur pour sélectionner l'utilisateur que vous désirez exporter.
2. Dans le menu du haut de la fenêtre de droite, cliquez sur **Export**. La fenêtre suivante va apparaître.

NOTES



Exporter

Serveur	Cybiolab.lan
Base DN	<input type="text" value="uid=drobbins,ou=Users,dc=cybiolab,dc="/> 
Portée de la recherche	<input checked="" type="radio"/> Base (dn de base seulement) <input type="radio"/> One (un niveau au-dessous de la base) <input type="radio"/> Sub (sous-arborescence entière)
Filtre de recherche	<input type="text" value="(objectClass=*)"/>
Afficher les attributs	<input type="text" value="*"/>
	<input type="checkbox"/> Inclure les attributs système
	<input checked="" type="checkbox"/> Enregistrer dans un fichier
	<input type="checkbox"/> Compress

Format d'exportation	Les lignes se finissent par
<input checked="" type="radio"/> LDIF	<input type="radio"/> UNIX (Linux, BSD)
<input type="radio"/> DSML V.1	<input type="radio"/> Macintosh
<input type="radio"/> VCARD 2.1	<input checked="" type="radio"/> Windows
<input type="radio"/> CSV (feuille de calcul)	

## NOTES



- Sélectionnez le *Serveur LDAP* désiré, dans le cas qu'il y aurait un Contrôleur de Domaine Secondaire (BDC).
- Vérifiez les informations suivantes:
  - Que vous avez le bon objet que vous désirez exporter;
  - Et que la zone de recherche d'exportation soit bien à *Base*.
  - Que la case *Enregistrer dans un fichier* soit coché. Si vous désirez que visualiser le résultat exporté ne cocher pas cette case.
  - Le format du fichier à sélectionner soit être de type *LDIF*.
  - Tandis que le format de fin de ligne du fichier LDIF doit être soit à *Unix* ou *Window*;

Pesez ensuite sur le bouton **Proceed**.

- Sélectionnez l'emplacement de sauvegarde en prenant soin d'enlever le *uid=* devant le nom.



