

## Création des groupes

La création des groupes est sûrement l'une des choses des plus importantes dans la gestion des utilisateurs et dans le mécanisme d'attribution des permissions pour les ressources.

Nous allons donc utiliser deux types de groupe dans notre projet:

- Les groupes Posix locaux;
- Les groupes Posix du domaine local;

Arrêtons-nous immédiatement. La convention de nommage des groupes que nous vous proposons ne s'applique pas vraiment à Linux. Il représente plus un dérivé de celle proposée par Windows. Il ne faut pas oublier que nous utilisons les services Samba avec un annuaire LDAP.

### Groupes Posix locaux

Le *groupe Posix local* ou simplement *groupe Posix* est applicable sur un ordinateur local uniquement et ne peut pas être utilisé par les autres ordinateurs du domaine.

Il fournira donc aux utilisateurs des permissions à des ressources partagées, situées seulement sur l'ordinateur local. Il permet aussi de fournir le droit d'effectuer différentes tâches, tel que d'exécuter des tâches planifiées, utiliser les périphériques (USB, CD-Rom, Floppy), de s'authentifier en tant que root, etc.

Il est important de comprendre que les groupes résident sur chacun des ordinateurs, dans le fichier group du répertoire /etc.

### Groupes Posix du domaine local

Le *groupe Posix du domaine local* est un groupe qui peut s'appliquer à tous les ordinateurs d'un même domaine. Le groupe Posix du domaine local est idéal pour donner les permissions sur des ressources réseaux que l'on désire partager.

Type de groupes recommandé sur un domaine Linux, ces groupes résident dans l'annuaire LDAP et peuvent par conséquent être utilisés par tous les ordinateurs du domaine.

NOTES









## Groupes Posix Locaux

Les groupes Posix locaux peuvent être utilisés pour donner des autorisations de ressources uniquement sur le poste sur lequel ce groupe existe. Il est donc impossible de le partager entre plusieurs ordinateurs du domaine. Pour une meilleure gestion, nous vous conseillons d'utiliser le plus possible les groupes Posix de Domaine.

Cependant, il arrive parfois des situations, que l'utilisation de groupes Posix locaux soient indispensables, par exemple avec les outils de gestion des bases de donnée Oracle 10g. Pour cette raison, nous allons vous montrer comment créer des groupes Posix locaux.

Traditionnellement les entrées des groupes sont emmagasinées dans le fichier *group* situé dans le répertoire */etc*. Ce fichier est un simple fichier texte comprenant une série d'entrées. Ces entrées se composent de différents champs séparés par des ":" :

```
nom_du_groupe:mot_de_passe:numéro_du_groupe:membre1,membre2
```

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

```
vim /etc/group
```

ou encore sous Gentoo.

```
vigr
```

Pour connaître les groupes dans lequel fait parti un utilisateur en particulier, saisir la commande suivante dans une console.

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

Par exemple, prenons l'utilisateur *root*.

```
id root
```

```
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),  
4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
```

NOTES



## Création d'un groupe Posix Local

L'outil de gestion Web phpLDAPAdmin, ne nous permet pas de créer des groupes Posix Locaux. Cependant les outils de base de Linux le peuvent. Pour ce faire, utiliser l'outil *groupadd*.

Pour créer un groupe Posix local

1. Ouvrez une console sur l'ordinateur dont vous désirez créer le groupe. Assurez-vous d'avoir ouvert une session sous l'utilisateur root.

**su -**

2. Puis saisissez la commande d'ajout d'un groupe supplémentaire.

**groupadd -g 1337 secretariat**

Il est important de comprendre que le numéro d'un groupe local (GID) va entrer en conflit avec le numéro d'un groupe du Domaine. Une stratégie de groupe reste donc indispensable.

## Suppression d'un groupe Posix local

Pour supprimer un groupe Posix local

1. Ouvrez une console sur l'ordinateur dont vous désirez supprimer le groupe.
2. Puis saisissez la commande.

**groupdel secretariat**

## Ajout de membres à un groupe Posix local

Pour ajouter un membre à un groupe Posix local

1. Ouvrez une console sur l'ordinateur dont vous désirez modifier l'appartenance d'un groupe.
2. Puis saisissez la commande pour ajouter un utilisateur dans un groupe supplémentaire.

**useradd -G secretariat utilisateur1**

NOTES



## Groupes Posix du Domaine

Les groupes Posix du Domaine sont utilisés pour donner des autorisations aux ressources sur le domaine. Il est donc facilement de le partager entre plusieurs ordinateurs d'un même domaine.

Les entrées des groupes sont emmagasinées dans l'annuaire LDAP de votre domaine. Cette centralisation facilitera la gestion des groupes pour les ordinateurs du domaine ainsi que pour l'autorisation sur les ressources.

Tout comme avec les groupes Posix locaux, pour connaître les groupes dans lesquels fait parti un utilisateur, il suffit simplement de saisir la commande suivante dans une console.

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

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

```
getent group
```

### Création d'un groupe Posix du domaine

1. Ouvrez l'outil web phpLDAPAdmin.
2. Dans le volet de gauche, cliquer sur le plus de l'unité organisationnel Groups.
3. Puis cliquer sur "*Create new entry here*".
4. Choisissez "*Domain Group*".
5. Vous devez maintenant entrer des valeurs aux attributs pour la création de votre groupe.

Le champ **Container DN** va vous permettre de spécifier l'emplacement où sera situé votre groupe dans l'arborescence LDAP. Cet entré devrait pointer sur l'unité d'organisation *ou=Groups* ou un de ses sous-unités de votre domaine.

Le bouton **Browse** va vous permettre de naviguer dans l'arborescence afin de choisir le bon emplacement de création. Encore ici, cliquer seulement sur les "plus" pour exploser une sélection.

NOTES



Entrons ensuite le **Group name**. Ne mettez pas d'espace lors de l'inscription du nom. L'outil phpLDAPAdmin et l'annuaire LDAP supporte les espaces, mais cela peut vous causer des ennuis pour les autorisations ou pour la gestion en ligne de commande.

Le champ **GID of group** doit contenir un numéro d'identification de groupe unique dans l'annuaire LDAP. Il est cependant possible de faire un chevauchement de GID entre celui contenu dans LDAP et celui contenu localement sur un ordinateur Linux.

Le champ **Description** est simplement à titre indicatif. Par défaut, le modèle affiche "Domain Group".

Dans le champ **Members**, ajouter la ou les personnes faisant parti de ce groupe. Si il vous manque des champs pour les noms, créer votre groupe et faites des ajouts de membre plus tard.

6. Appliquer votre demande.

### Ajout de membres à un groupe Posix du domaine

Pour ajouter un membre à un groupe Posix du domaine

1. Ouvrez une l'outil web phpLDAPAdmin.
2. Puis naviguer dans l'arborescence LDAP jusqu'à votre groupe dont vous désirez ajouter l'utilisateur.

Si c'est le premier utilisateur que vous entrez dans le groupe, dans le volet de droit, cliquer sur **Add new attribute**.

Dans la liste déroulante, choisissez *memberUid* et entrez le nom de l'utilisateur dans le champ vide à sa droite.

Si le groupe contient déjà au moins un utilisateur, rechercher le champ *memberUid* et cliquer sur **Add value**. Entrez simplement votre nouveau membre et appliquer le changement.



**NOTE:** il n'y a pas de vérification de nom d'utilisateur. Vous pouvez donc entrer des utilisateurs inexistant dans ces champs. A vous de s'assurer de la bonne syntaxe des noms.

3. Assurez-vous d'appliquer les modifications en cliquant sur **Save Changes**.

NOTES







- 9 Enfin, dans le champ "Users", entrer vos utilisateurs appartenant au groupe.

NOTES



## Création des groupes systèmes du domaine.

Pour vous aidez, voici un fichier LDIF, vous permettant de créer rapidement les correspondances les plus utilisées. N'oubliez pas de remplacer le SID de Domaine par celui de votre Domaine.

Créer un fichier **baseGroups.ldif** contenant les entrées suivantes:

```
dn: cn=DomainAdmins,ou=System,ou=Groups,dc=cybiolab,dc=lan
cn: DomainAdmins
displayName: Domain Admins
sambaSID: S-1-5-21-1234567890-123456789-1234567890-512
memberUid: root
objectClass: posixGroup
objectClass: sambaGroupMapping
objectClass: top
gidNumber: 0
sambaGroupType: 2

dn: cn=DomainUsers,ou=System,ou=Groups,dc=cybiolab,dc=lan
cn: DomainUsers
displayName: Domain Users
sambaSID: S-1-5-21-1234567890-123456789-1234567890-513
objectClass: posixGroup
objectClass: sambaGroupMapping
objectClass: top
gidNumber: 100
sambaGroupType: 2

dn: cn=DomainGuest,ou=System,ou=Groups,dc=cybiolab,dc=lan
cn: DomainGuest
displayName: Domain Guest
sambaSID: S-1-5-21-1234567890-123456789-1234567890-514
objectClass: posixGroup
objectClass: sambaGroupMapping
objectClass: top
gidNumber: 65534
sambaGroupType: 2

dn: cn=DomainComputers,ou=System,ou=Groups,dc=cybiolab,dc=lan
cn: DomainComputers
displayName: Domain Computers
sambaSID: S-1-5-21-1234567890-123456789-1234567890-515
objectClass: posixGroup
objectClass: sambaGroupMapping
```

```

objectClass: top
gidNumber: 65533
sambaGroupType: 2

dn: cn=ServerOperators,ou=System,ou=Groups,dc=cybiolab,dc=lan
cn: ServerOperators
displayName: Serveur Operators
gidNumber: 549
sambaGroupType: 2
objectClass: posixGroup
objectClass: sambaGroupMapping
objectClass: top
sambaSID: S-1-5-21-1234567890-123456789-1234567890-549

dn: cn=PrintOperators,ou=System,ou=Groups,dc=cybiolab,dc=lan
cn: PrintOperators
displayName: Print Operators
gidNumber: 550
sambaGroupType: 2
objectClass: posixGroup
objectClass: sambaGroupMapping
objectClass: top
sambaSID: S-1-5-21-1234567890-123456789-1234567890-550

```

Puis, ajouter ces entrées dans votre annuaire LDAP. Vous pouvez utiliser la commande suivante, ou réutilisé le script *import\_Idif.sh* créer antérieurement.

```
/usr/bin/ldapadd -x -D "cn=root,dc=cybiolab,dc=lan" -W -f mapping.ldif
```

ou

```
./import_Idif.sh baseGroups.ldif
```

Pour faire une vérification, allez dans votre outil web phpLDAPAdmin ou encore, saisissez en console la commande,

```
net groupmap list
```

NOTES

