Utilisateurs et Groupes

Stage personnes ressources réseau en établissement
janvier 2005

Formateurs : Jackie DAÖN

Médiapôle de Guyancourt Lycée de Villaroy – 2 rue Eugène Viollet Le Duc – BP31 – 78041 GUYANCOURT Cedex
Tel : 01 30 48 91 88 / Fax : 01 30 57 49 70 – www.mp-guyancourt.ac-versailles.fr
Jackie.Daon@crdp.ac-versailles.fr

Sommaire

Gestion des comptes d'utilisateurs

Un compte d'utilisateur de domaine donne la possibilité d'ouvrir une session sur le domaine pour accéder aux ressources du réseau, ou d'ouvrir une session sur un ordinateur pour accéder aux ressources de cet ordinateur.

Un groupe est un ensemble de comptes d'utilisateurs. Vous pouvez utiliser des groupes pour gérer efficacement l'accès aux ressources du domaine, ce qui simplifie la maintenance et l'administration du réseau.

Comptes d'utilisateurs locaux et de domaine

Les comptes d'utilisateurs locaux résident sur la machine locale. Les comptes locaux ne peuvent pas accéder à des ressources de domaine Windows 2003 et ne devraient pas être créés sur des machines qui font parties d'un domaine.

Les comptes d'utilisateurs de domaine résident dans Active Directory, sur des contrôleurs de domaine et peuvent accéder à toutes les ressources sur le réseau, à condition d'avoir les privilèges nécessaires.

Les comptes prédéfinis sont : Administrateur et Invité (désactivé par défaut).

Les types de comptes

Comptes locaux

Ils sont créés par l'intermédiaire de la console de Gestion de l'ordinateur.
Les comptes locaux ont la particularité d'être enregistrés dans la base de données de comptes locale : la SAM.
Ils ne sont pas enregistrés dans Active Directory.
Il est déconseillé de créer des comptes locaux sur des machines rattachées à un domaine, car les utilisateurs n'auront accès qu'aux ressources locales de la machine.

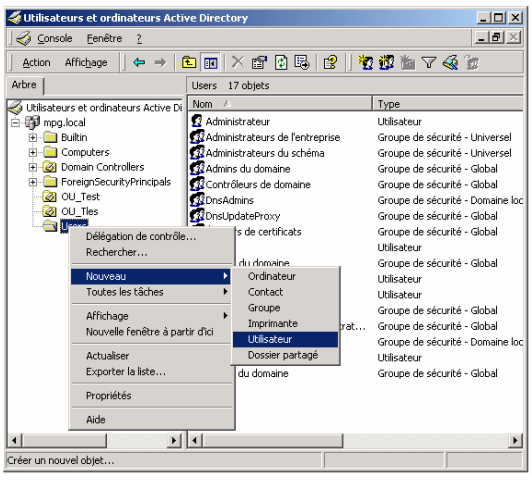
Comptes de domaine

Les comptes d'utilisateurs de domaine résident dans Active Directory, sur des contrôleurs de domaine et peuvent accéder à toutes les ressources sur le réseau, à condition d'avoir les privilèges nécessaires.
Dans ce cas, l'utilisateur peut ouvrir une session à partir de tout poste du domaine (sauf interdictions particulières).

Création d'un compte utilisateur

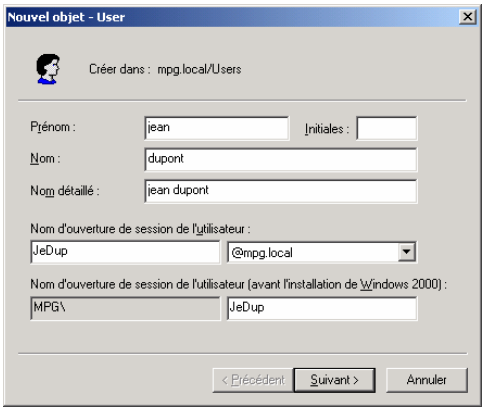
La procédure suivante permet de créer le compte utilisateur **Jean Dupont**

Pour créer un nouveau compte utilisateur utilisez la console **Utilisateurs et ordinateurs Active Directory**.
1. Cliquez avec le bouton droit sur **Nouveau**, puis sur **Utilisateur**, ou utilisez le bouton **Nouvel utilisateur** dans la barre d'outils.



2. Tapez les informations utilisateur :
Prénom : Jean
Nom : Dupont
Nom d'utilisateur : JeDup

3. Cliquez sur **Suivant**



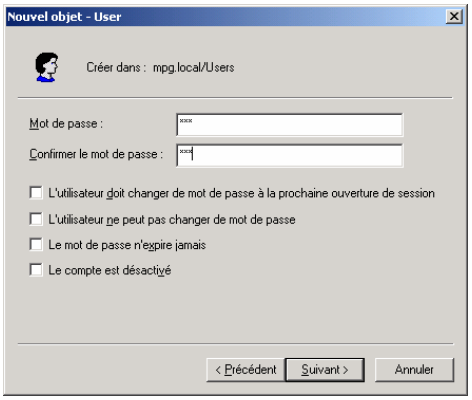
4. L'assistant vous demande ensuite de saisir le mot de passe et ses propriétés.

L'utilisateur doit changer de mot de passe à la prochaine session. Cela lui donne la responsabilité du mot de passe, une fois son compte créé.

L'utilisateur ne peut pas changer de mot de passe.

Le mot de passe n'expire jamais. Le délai d'expiration du mot de passe peut être paramétré, pour forcer les utilisateurs à en changer régulièrement.

Le compte est désactivé. En cas d'absence durable d'un utilisateur ou changement d'année scolaire. Évite de recréer des comptes (les permissions devraient aussi être recréées !). Ou compte servant de modèle à la création d'autres comptes
Entrez un mot de passe dans les zones **Mot de passe** et **Confirmer le mot de passe** et sélectionnez les options de compte appropriées.



5. Acceptez la boîte de dialogue de confirmation.

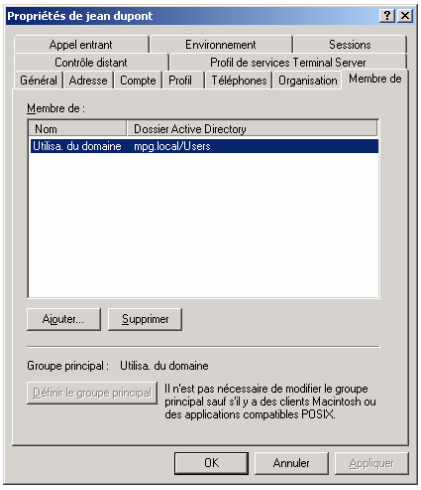
Vous venez de créer un compte pour Jean Dupont.

Un utilisateur est obligatoirement membre d'un groupe d'utilisateurs.

Par défaut, il est membre du groupe Utilisateurs du Domaine. Pour le vérifier, clic droit sur son nom / Propriétés / Membre De

Un utilisateur peut être membre de plusieurs groupes.

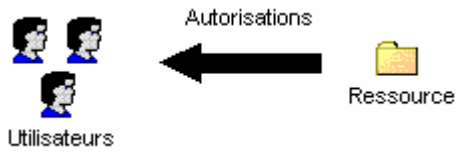
Vous pouvez créer des groupes d'utilisateurs, d'ordinateurs, etc., et des groupes composés de plusieurs classes d'objets (utilisateurs + ordinateurs, etc.)



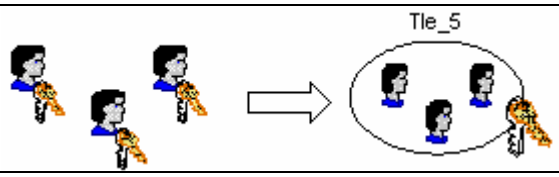
Gestion des groupes dans un domaine

Les groupes de Windows 2003 sont utilisés pour gérer les comptes d'utilisateurs dans le but d'accéder à des ressources. Tout ceci dans un souci de simplifier l'administration. Il est en effet plus aisé d'utiliser un groupe en fonction du besoin, plutôt que de sélectionner plusieurs utilisateurs éparpillés dans une liste de comptes. Les groupes peuvent bénéficier de droits particuliers (comme par exemple le droit de sauvegarder, de gérer les imprimantes, etc ...) ou hériter des droits par imbrication du groupe dans un autre groupe.
Active Directory apporte quelques nouveautés dans la notion de groupe par rapport à NT 4.

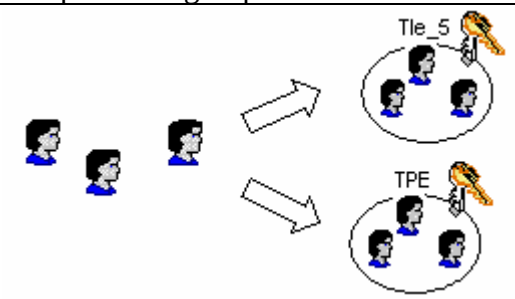
Puisqu'un objet hérite automatiquement des droits de son parent, il est intéressant de former des groupes, d'y placer des objets, et d'attribuer des permissions aux groupes. Cela évite de traiter chaque objet séparément.

Sur les ressources, on définit les autorisations (droits Lecture, Ecriture, Modifier, …) que l'on veut affecter à certains utilisateurs ou groupes.	

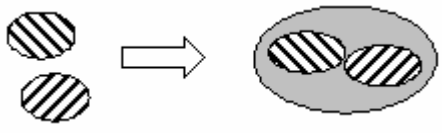
- Les groupes simplifient l'affectation d'autorisations à des ressources :

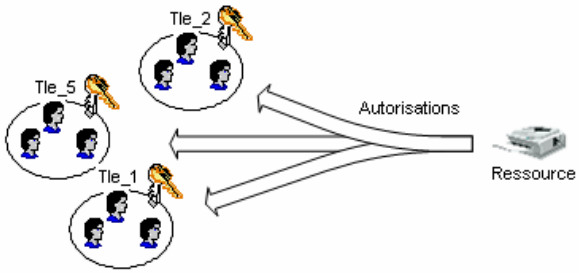
On peut ainsi former un groupe « Tle_5 » qui est le seul à avoir accès à un dossier défini. Il suffit de placer dans ce groupe tous les élèves de cette classe.	

- Les utilisateurs peuvent être membres de plusieurs groupes :

On peut ainsi placer les mêmes utilisateurs dans des groupes différents. L'élève Jean Dupont est dans le groupe Tle_5, mais il est également dans le groupe TPE.	

- Les groupes peuvent être imbriqués dans d'autres groupes

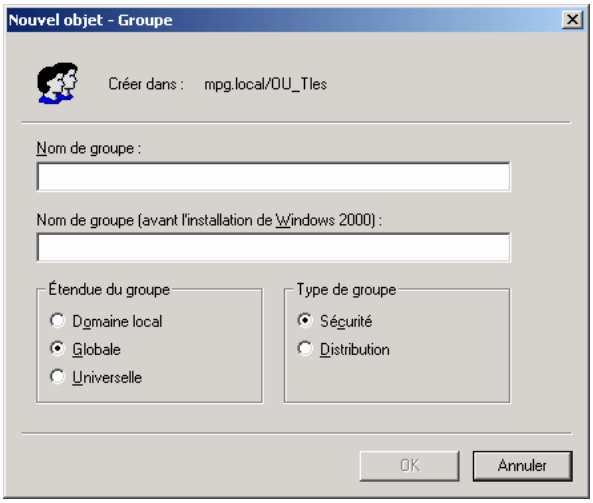
On peut même imbriquer des groupes (les groupes Tle_1, Tle_2, etc… appartiennent à un même groupe appelé « Terminales » qui est seul à avoir accès à un dossier « Terminales »)	

On peut attribuer des autorisations d'une même ressource à plusieurs groupes (ex : l'imprimante est accessible aux groupes Tle_1, Tle_2, … Tle_5, mais pas aux autres élèves.	

Types de groupe

Deux types de groupes sont disponibles :

- les **groupes de sécurité** utilisés pour gérer la sécurité des ressources du ou des domaines.
- les **groupes de distribution** utilisés par exemple pour envoyer des messages électroniques à l'ensemble des utilisateurs de ces groupes. Ces groupes ne peuvent pas être utilisés pour la sécurité. Des applications comme Exchange 2003 s'appuient sur la base d'annuaire Windows 2003 et peuvent ainsi utiliser les groupes de distribution.



Ces deux types de groupes possèdent une étendue qui spécifie les comptes qui peuvent en faire partie ainsi que l'endroit où ils peuvent être utilisés.

Étendues de groupe

L'étendue d'un groupe définit les restrictions d'appartenance et d'utilisation du groupe. Il existe trois étendues différentes applicables aux groupes de sécurités :

- **Groupes globaux**
  Ces groupes peuvent être utilisés pour accorder un accès à des ressources dans n'importe quel domaine de la forêt et ils servent généralement à regrouper des utilisateurs ayant des besoins similaires en termes d'accès aux ressources.

- **Groupes locaux de domaine**
  Ces groupes ne peuvent être utilisés que pour un accès à des ressources du domaine local.

- **Groupes universels**
  Ces groupes peuvent être utilisés pour accéder à des ressources dans n'importe quel domaine de la forêt. Ils diffèrent des groupes globaux par le fait qu'ils ne sont disponibles que dans les domaines WS2003 s'exécutant en mode natif. De plus, leurs membres peuvent provenir de n'importe quel domaine, alors que ceux des groupes globaux ne peuvent provenir que du propre domaine du groupe. Les groupes universels sont nouveaux dans WS2003 et n'ont pas d'équivalence sous NT.

Les propositions d'étendue du groupe diffèrent selon le mode de configuration du domaine mode natif ou mode mixte. Lorsque la migration de tous les contrôleurs de domaine antérieurs à Windows 2000 est effectuée, vous pouvez basculer en

mode natif. Vous pourrez alors utiliser les groupes universels, ainsi que l'imbrication de groupes dans d'autres groupes.

Pour modifier le mode de configuration du domaine, utilisez la console Utilisateurs et ordinateurs Active Directory, affichez les Propriétés du domaine et cliquez sur **Augmenter le niveau fonctionnel du domaine...**

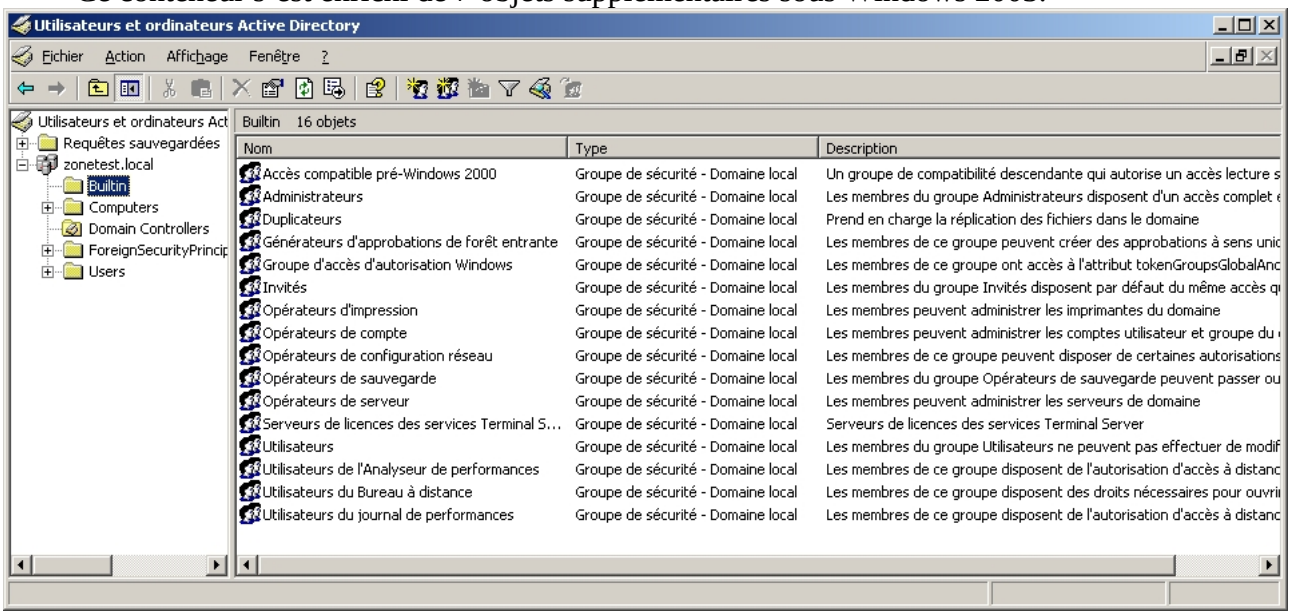
Les différents groupes

Les groupes prédéfinis

Sur tous les ordinateurs fonctionnant sous Windows 2003, un certain nombre de groupes prédéfinis sont créés lors de l'installation de Windows 2003 :

- les **groupes locaux prédéfinis** que vous retrouvez dans le conteneur ***Builtin***.
- les **groupes globaux prédéfinis** ainsi que certains **groupes de domaine local** qui se créent dans le conteneur ***Users***.

Builtin réunit les groupes prédéfinis du domaine avec une étendue de domaine local. Ce conteneur s'est enrichi de 7 objets supplémentaires sous Windows 2003.



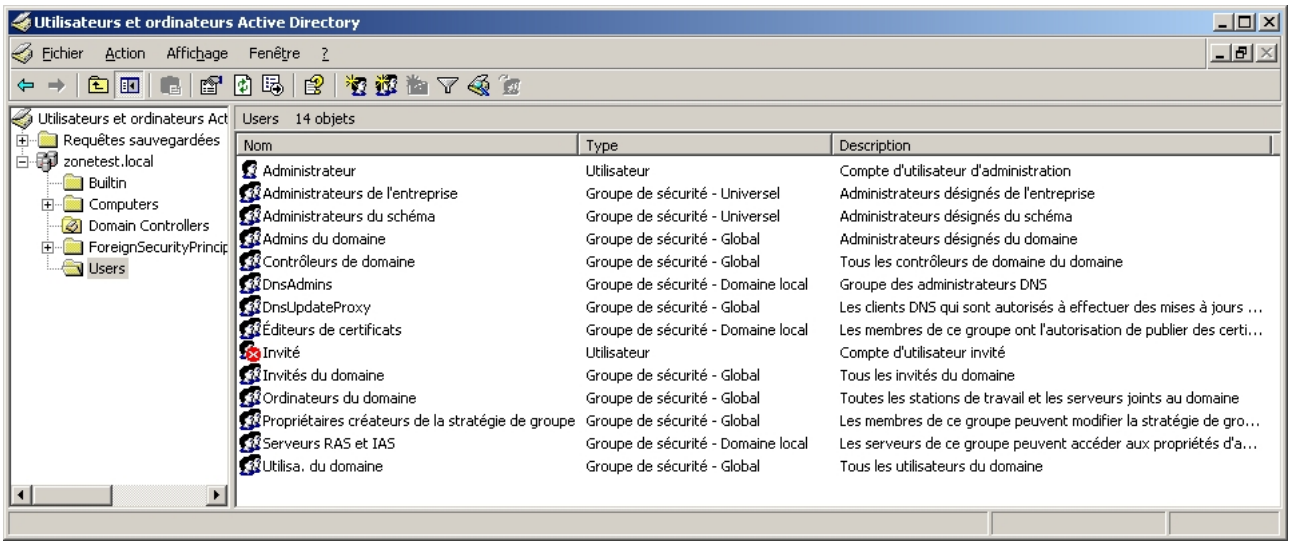
Ces groupes disposent de droits et de permissions implicites ; aussi en insérant un membre dans un de ces groupes, vous lui octroyez des droits supplémentaires.

Opérateurs de compte	Les membres de ce groupe peuvent administrer les comptes d'utilisateurs et groupes (ajouter, supprimer et modifier). Ils ne peuvent cependant pas toucher au compte Administrateur ni aux autres membres du groupe Opérateurs de compte.
Opérateurs de serveur	Les membres de ce groupe peuvent partager des ressources ainsi qu'effectuer des sauvegardes et des restaurations sur des contrôleurs de domaine.
Opérateurs d'impression	Les membres de ce groupe peuvent gérer les imprimantes réseau des contrôleurs de domaine.
Administrateurs	Les membres de ce groupe peuvent administrer les contrôleurs de domaine ainsi que toute station ayant intégrée le domaine. Par défaut, le groupe global Administrateurs de domaine ainsi que le compte Administrateur font partie du groupe local Administrateurs.
Invité	Le groupe global Invités du domaine ainsi que le compte d'utilisateur Invité sont intégrés dans ce groupe. Les membres de ce dernier disposent de peu de droits.

Opérateurs de sauvegarde	Les membres de ce groupe peuvent effectuer des sauvegardes et restaurations sur tout contrôleur de domaine.
Utilisateurs	Le groupe global du domaine utilisateur est intégré dans ce groupe. Ce groupe peut être utilisé pour affecter des droits et permissions à toute personne disposant d'un compte dans le domaine.
Duplicateurs	Le groupe local Duplicateurs effectue les réplications de répertoires. Le compte d'utilisateur de ce groupe est configuré afin de se connecter au service Duplicateur du contrôleur de domaine
Accès compatible Pré-Windows 2000	Ce groupe permet de faire fonctionner les applications avec un niveau de sécurité Windows 2000 ou de version antérieure à Windows 2000.

Par défaut, les différents groupes opérateurs ne disposent pas de membres. Ajoutez des comptes d'utilisateurs dans ceux-ci pour attribuer des droits spécifiques à vos utilisateurs. Si un utilisateur est désigné pour effectuer les sauvegardes, alors intégrez-le dans le groupe Opérateurs de sauvegarde plutôt que dans le groupe Administrateurs. II est préférable de limiter les droits d'un utilisateur à ses fonctions pour une question de maîtrise de la sécurité.

Le conteneur ***Users*** liste les groupes prédéfinis du domaine avec une étendue globale ainsi que quelques groupes prédéfinis du domaine avec une étendue de domaine local.



Par imbrication de groupe, l'appartenance à des groupes avec une étendue globale offre aussi des droits particuliers dans le domaine.

Invités du domaine	Le compte d'utilisateur **Invité** est automatiquement intégré à ce groupe. De plus, ce groupe global est lui aussi automatiquement intégré dans le groupe local du domaine **Invités**.
Utilisateurs du domaine	Tous les comptes d'utilisateurs que vous créez font partie de ce groupe. Ils ne peuvent effectuer que des tâches que vous avez spécifiées et n'ont accès qu'aux ressources auxquelles vous avez attribué des permissions. Ce compte est automatiquement intégré au groupe local du domaine **Utilisateurs**. Tout utilisateur créé dans le domaine est automatiquement inséré dans ce groupe
Administrateurs du domaine	Le compte administrateur fait partie de ce groupe, qui est intégré au groupe local du domaine **Administrateurs**. En fait, le compte d'utilisateur Administrateur ne possède pas de droit particulier en tant que compte. C'est le fait de l'intégrer dans ce groupe global qui lui-même fait partie du groupe local du domaine Administrateur qui lui donne ses droits.

Administrateurs de l'entreprise	Les personnes membres de ce groupe disposent de droits d'administrateur sur tout le réseau (et non pas limité au domaine).
Administrateurs du schéma	Les membres de ce groupe sont habilités à modifier le schéma c'est-à-dire à définir de nouvelles classes et de nouveaux attributs pour les classes existantes.
Contrôleurs de domaine	Ce groupe contient les comptes d'ordinateur contrôleurs de domaine du domaine.

Les groupes spéciaux

II existe aussi les groupes spéciaux Windows 2003 qui ne peuvent pas se manipuler. En effet, la qualité de membre de ces groupes ne peut pas être modifiée et fait référence à l'état de votre système à un instant donné.

Ce sont les groupes **Tout le monde**, **Utilisateurs authentifiés**, **Créateur propriétaire**, **Réseau**, **Interactif**…

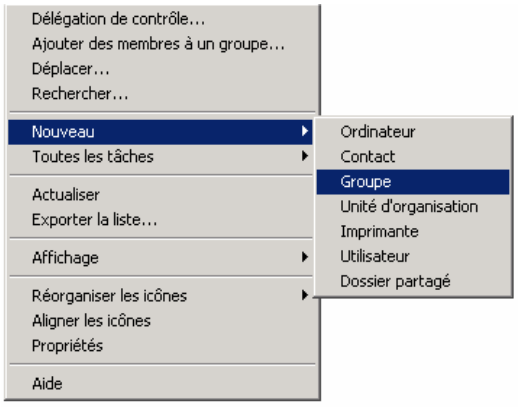
- Le groupe **Tout le monde** : comprend tous les utilisateurs, ceux que vous avez créés, le compte Invité ainsi que tous les utilisateurs des autres domaines. ***Attention, car lorsque vous partagez une ressource, ce groupe dispose par défaut de la permission Lecture sur le partage (et Contrôle total sous Windows 2000 !).***.
- Le groupe **Utilisateurs authentifiés** : comprend tout utilisateur possédant un compte d'utilisateur et un mot de passe pour la machine locale ou Active Directory. ***Affectez des permissions à ce groupe plutôt qu'au groupe Tout le monde.***
- Le groupe **Créateur propriétaire** : toute personne ayant créé ou pris possession d'une ressource, fait partie de ce groupe pour la ressource concernée. Le propriétaire d'une ressource dispose des pleins pouvoirs sur cette dernière.
- Le groupe **Réseau** : comprend toute personne accédant via le réseau à une ressource.
- Le groupe **Interactif** : comprend tous les utilisateurs qui ont ouvert une session localement (dans le cas où vous utilisez Terminal Server, ce groupe comporte tous les utilisateurs ayant ouvert une session sur le serveur de terminal).

Les groupes manuels

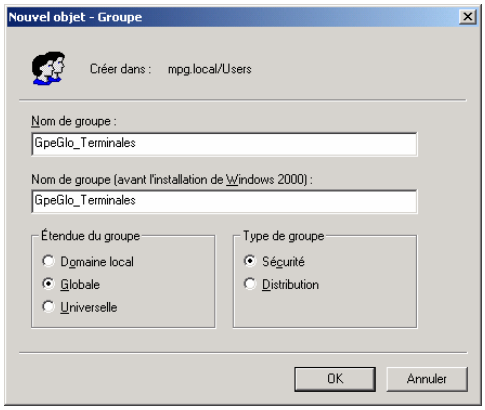
Bien évidemment, vous avez la possibilité de créer manuellement des groupes du type Sécurité ou Distribution, d'étendue Domaine local, Globale ou Universelle.

Pour créer ces groupes, utilisez la console **Utilisateurs et ordinateurs Active Directory**.

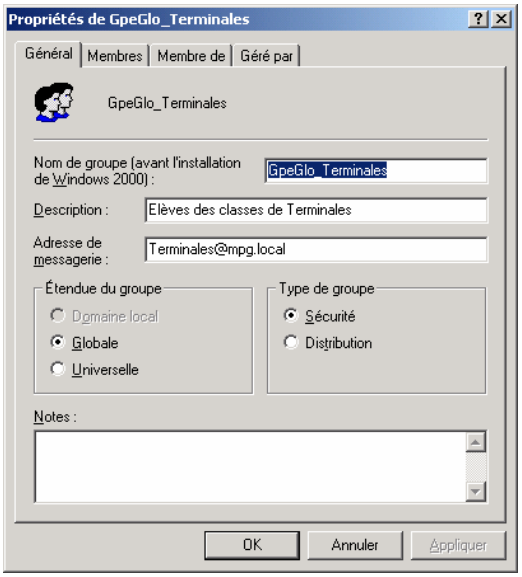
Faites un clic droit sur l'unité d'organisation dans laquelle vous souhaitez créer votre groupe. cliquez sur **Nouveau** puis sélectionnez **Groupe**.



Sélectionnez le type et l'étendue du groupe et donnez lui un nom significatif (63 caractères au maximum).
Le nom d'un groupe est unique sur le domaine
Il ne peut pas être celui d'un utilisateur existant



L'onglet **Membres** permet de visualiser, d'ajouter ou de supprimer des comptes d'utilisateurs, d'ordinateurs ou un autre groupe.
L'onglet **Membre de** permet d'afficher la liste des groupes dont ce groupe fait partie. Par ce biais, vous pouvez aussi insérer ce groupe dans un autre groupe.
L'onglet **Géré par** permet d'afficher les coordonnées de la personne ou du groupe (complétées dans les propriétés du compte) qui est chargé de gérer le groupe



- Un groupe peut être **déplacé** librement dans un domaine.
- Un groupe peut être **renommé**
- Un groupe peut être **supprimé.**
  La suppression d'un groupe ne supprime pas ses membres.
  Attention à la suppression des groupes locaux qui risque de rendre certaines ressources inaccessibles !

Imbrication des groupes dans Active Directory

L'imbrication des groupes autorise l'ajout de compte d'utilisateurs, d'ordinateurs ou de groupes dans un autre groupe. Il ne peut être membre d'un autre groupe.

En mode mixte

- Un groupe **Local de domaine** peut contenir des utilisateurs et groupes globaux de n'importe quel domaine.
- Un groupe **Global** peut contenir uniquement des utilisateurs du même domaine que le sien.
- II n'existe pas de groupe **Universel** en mode mixte.

En mode natif ou Windows 2003 server

- Un groupe **Local de domaine** peut contenir des comptes d'utilisateurs, des groupes globaux et des groupes universels de n'importe quel domaine de la forêt, ainsi que des domaines locaux de son propre domaine. Mais il ne peut être membre d'un autre groupe.
- Un groupe **Global** peut contenir des comptes d'utilisateurs et des groupes globaux uniquement du même domaine.

- Un groupe **Universel** peut contenir des comptes d'utilisateurs, des groupes globaux et des groupes universels de n'importe quel domaine de la forêt.

Le groupe local de domaine peut être utilisé pour mettre des permissions sur des ressources de son domaine : il n'est visible que dans son propre domaine.
Les groupes globaux et universels peuvent être utilisés pour définir des permissions sur des ressources à partir de n'importe quel domaine de la forêt. Ils sont visibles dans tous les domaines de la forêt.
Il n'est pas possible de créer des groupes imbriqués dans des domaines en mode mixte. Un groupe imbriqué est donc un groupe membre d'un autre groupe.
Un groupe imbriqué hérite automatiquement les permissions de son groupe parent et peut également disposer de permissions spécifiques. L'imbrication de groupes peut faciliter leur gestion à condition qu'elle soit planifiée avec soin.

Pour imbriquer des groupes, il suffit de sélectionnez le groupe qui deviendra le groupe enfant et de l'ajouter en tant que membre du groupe choisit comme groupe parent. Le groupe enfant apparaît dans l'onglet Membres.

Imbrication possible des groupes

Étendue	**Peut être imbriqué dans**		
	Global	**Domaine local**	**Universel**
Global	Oui (uniquement depuis le même domaine)	Oui	Oui
Domaine local	Non	Non	Non
Universel	Non	Oui	Oui

Convertir des étendues
Windows 2003 server permet de convertir un type d'étendue de groupe en une autre. Cela apporte une souplesse plus important que sous NT. Cependant, le passage des groupes d'une étendue à une autre ne peut se faire que dans des domaines dont le niveau fonctionnel de domaine est Windows 2000 natif ou Windows Server 2003.

En résumé :

Étendue	**Peut être convertie en**		
	Globale	**Domaine local**	**Universelle**
Globale	Non	Non	Oui
Domaine local	Non	Non	Oui
Universelle	Oui	Oui	Non

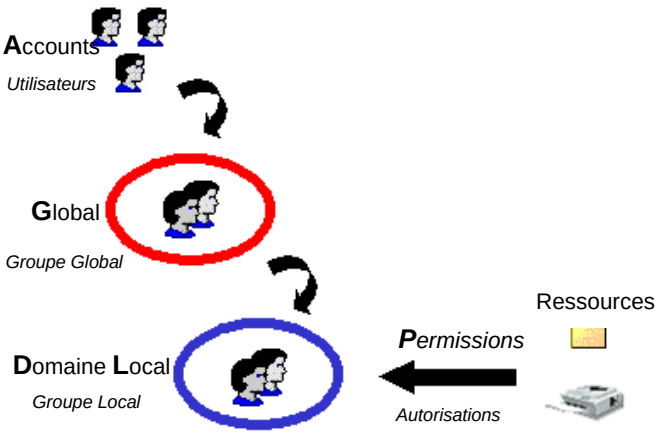
Stratégie d'utilisation des groupes dans un domaine

Microsoft recommande plusieurs combinaisons de stratégie d'utilisation de groupe
C G DL A ou **C G G DL A**
ou bien **C G U DL A** ou **C G G U DL A**.

C	Compte	Compte d'utilisateur
G	Global	Groupe d'étendue globale
DL	Domain Local	Groupe d'étendue domaine locale
A	Autorisations	Autorisation ou refus attribués à un compte ou un groupe sur une ressource
U	Universel	Groupe d'étendue universelle

Conseil : Un groupe local ne pouvant bénéficier d'autorisations que pour le domaine dans lequel il existe, essayez, dans la mesure du possible, d'organiser les utilisateurs à l'aide des groupes globaux, puis intégrez ces groupes globaux (qui peuvent provenir de n'importe quel domaine de la forêt) dans les groupes locaux. Affectez ensuite les permissions sur les ressources aux groupes locaux, ce qui propagera automatiquement ces permissions aux utilisateurs membres des groupes globaux.

A G DL P



Les Unités Organisationnelles

Une unité organisationnelle (UO) est un conteneur logique utilisé pour regrouper des objets d'un domaine a des fins de sécurité et d'administration. Il est possible de créer des structures arborescentes hiérarchiques d'UO afin de reproduire la structure géographique, organisationnelle ou administrative de votre domaine ou forêt.

Il ne faut pas confondre les unités organisationnelles avec des groupes d'utilisateurs !

Les unités organisationnelles accueillent des utilisateurs, des ordinateurs et des groupes.

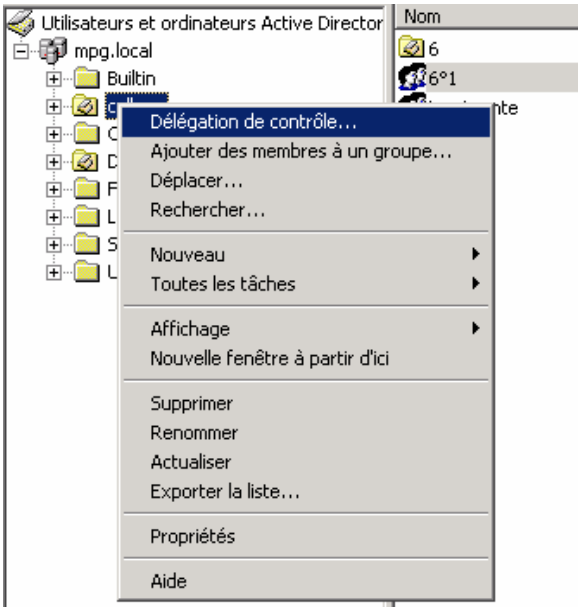
Elles permettent de mieux refléter la structure fonctionnelle de l'établissement.

Il est possible d'en déléguer de façon plus ou moins complète l'administration.

Les unités organisationnelles peuvent être imbriquées.

Les objets peuvent être déplacés à l'aide de l'option Déplacer du clic droit.

Les sélections multiples sont acceptées.



- Un objet ne peut exister que dans une seule unité organisationnelle.
- La suppression s'effectue par un simple clic droit, option supprimer.
  La suppression d'une UO supprime également tous les objets qu'elle contient !!!

Les droits d'accès ne peuvent être accordés qu'à des principaux de sécurité, c'est à dire des comptes d'utilisateurs et des groupes de sécurité.
À la différence du service d'annuaire de Novell, NDS, Active Directory ne traite pas les unités d'organisation comme des principaux de sécurité. Vous ne pouvez pas accorder des droits à une unité d'organisation et vous attendre à ce que ces droits soient hérités par les utilisateurs et groupes qu'elle contient.
Si vous êtes un administrateur NDS, et que vous souhaitez appliquer cette fonctionnalité, la seule possibilité est de placer et d'organiser stratégiquement des groupes globaux. La méthode consiste en fait à créer un groupe global dans chaque unité d'organisation et à le nommer en fonction de l'unité. Il suffit ensuite d'inclure tous les utilisateurs et groupes dans l'unité en tant que membres du groupe global qu'elle contient. Il faut ensuite ajouter les groupes globaux des unités de niveau suivant. Ce système d'imbrication permet la propagation des droits tout le long de l'arbre. Accordez des droits aux groupes globaux de ces unités comme si vous les accordiez à l'unité d'organisation même.
L'architecture de ce système est illustrée ci-dessous.