

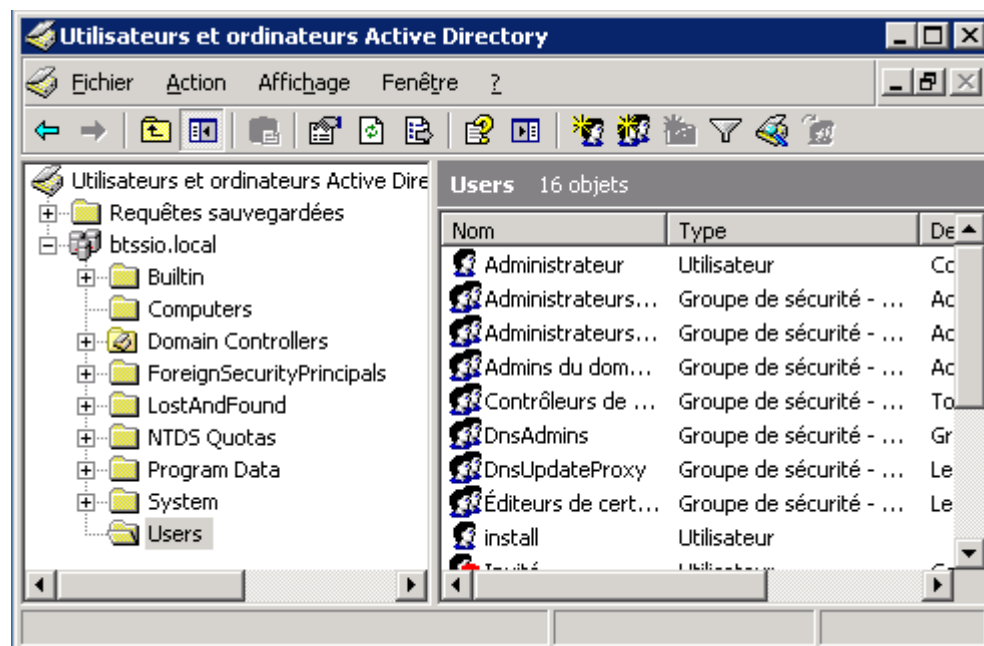
La gestion des utilisateurs et des ordinateurs

Active Directory permet de gérer plusieurs types d'objets :



La console Utilisateurs et ordinateurs Active Directory contient les dossiers suivants :

- Le dossier **Builtin** contient les groupes par défaut avec une étendue de domaine local.
- Le dossier **Computers** contient les comptes d'ordinateurs des stations clientes appartenant au domaine.
- Le dossier **Domain Controllers** contient les contrôleurs du domaine.
- Le dossier **Users** est le conteneur par défaut des utilisateurs du domaine.



Les profils d'utilisateurs

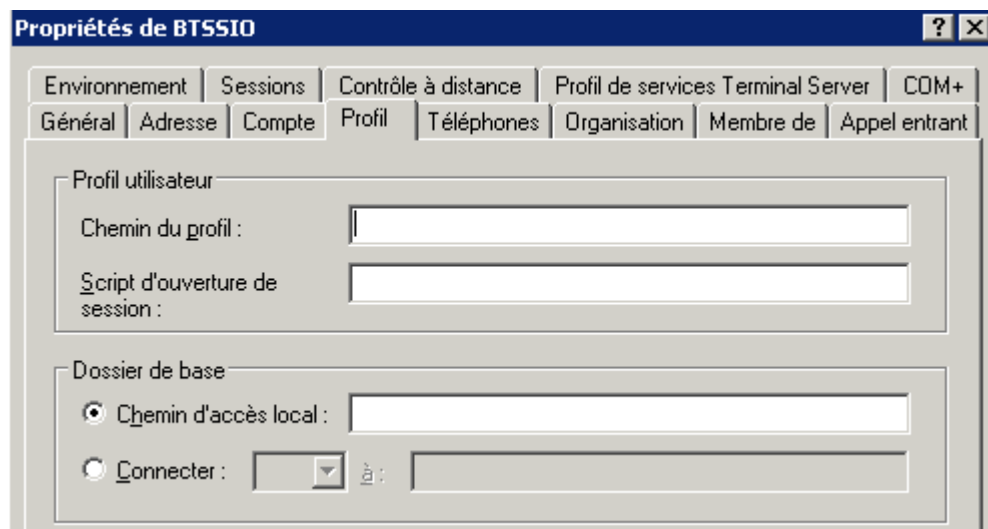
Un profil utilisateur contient tous les informations qui définissent l'environnement de travail d'un l'utilisateur.

- le fichier **ntuser.dat** contenant le profil dans le dossier **Documents and settings**,
- le profil est construit localement la première fois à partir du profil **Default user**,

Le profil errant : il s'agit de retrouver son profil sur n'importe quelle station. Pour cela il faut modifier les propriétés du compte en indiquant dans l'onglet Profil le **chemin réseau UNC** existant (utilisation de la variable **%username%** pour la création automatique du dossier **%%\\serveur\profiles\%username%%**).

Il est possible d'imposer un profil errant (obligatoire) en renommant **ntuser.dat** en **ntuser.man**.

Le **répertoire de base** (dossier personnel) peut être créé automatiquement en utilisant la variable **%username%** sur les partitions NTFS (Autorisation **Contrôle Total** pour l'administrateur et l'utilisateur).



Les groupes d'utilisateurs

Les groupes d'utilisateurs permettent de rassembler des utilisateurs devant bénéficier des mêmes droits ou autorisations. Il existe 2 types de groupe :

- les groupes de **sécurité** pour gérer l'accès aux ressources et que vous allez utiliser,
- les groupes de **distribution** (pour envoyer des messages à plusieurs utilisateurs avec le logiciel de messagerie Exchange).

Il y a 3 étendues de groupe :

- **Global** : pour organiser les comptes utilisateurs et avoir des autorisations dans tous domaines. Cela sert à regrouper des utilisateurs ayant des besoins similaires en termes d'accès aux ressources.(Ex. : le groupe **Utilisateurs du domaine**)
- **Domaine local** : pour définir des autorisations à des ressources du domaine local (Ex. : le groupe **Administrateurs**)
- * **Universelle** : pour regrouper les comptes d'utilisateurs de n'importe quel domaine et assigner des autorisations dans n'importe quel domaine.

Attention : les stations Windows ainsi que les serveurs Windows membre d'un domaine conservent une **gestion locale des comptes**, c'est à dire la gestion d'**utilisateurs locaux** et de **groupes locaux**.

La gestion d'un domaine peut se faire par **niveau de fonctionnalité** afin de pouvoir intégrer des serveurs « anciens » avec des serveurs plus « récents ». En mode natif

- il est possible d'**imbriquer des groupes dans d'autres groupes**, c'est à dire qu'un groupe peut être membre d'un autre groupe.
- un groupe domaine local contient des comptes, des groupes globaux et universel de tous les domaines + des groupes local du domaine.
- un groupe global contient des comptes et des groupes globaux du même domaine.
- Un groupe universel contient des compte, des groupes globaux et universels de tous les domaines.

Sous certaines conditions, il est possible de modifier l'étendue d'un groupe.

Les membres d'un groupe possèdent les **droits et autorisations** accordés au groupe.

Un utilisateur peut être membre de plusieurs groupes.

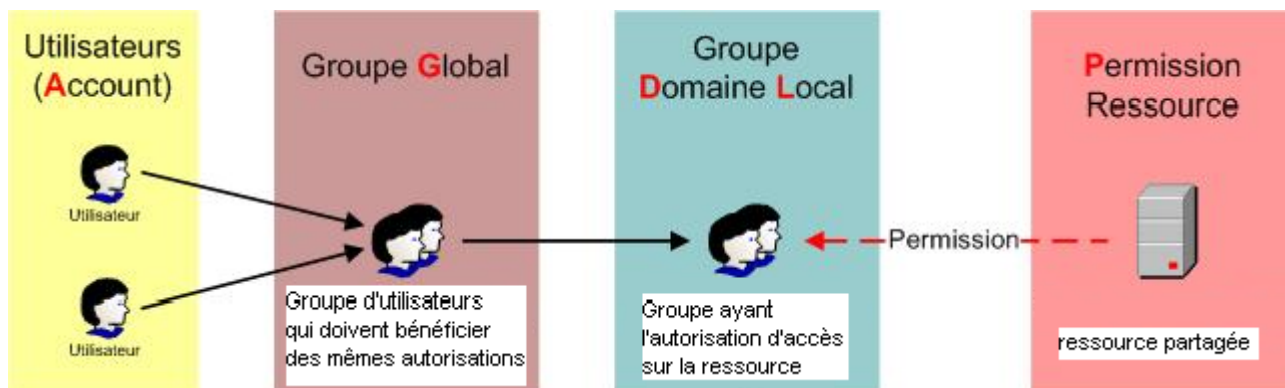
Démarche d'utilisation des groupes

Les groupes globaux reflètent l'organisation de l'entreprise.

Les groupes locaux de domaine sont à utiliser pour gérer les autorisations sur des ressources bien déterminées. Démarche préconisée par Microsoft (dans un contexte de domaine unique, sans forêt) :

AGDLP, qui signifie : **A**ccount, **G**lobal group, **D**omain Local group, **P**ermission.

On ne met pas d'autorisations d'accès directement sur les utilisateurs sauf si l'utilisateur est vraiment unique (dossier personnel / répertoire de base).



Exemple : dans une organisation, les utilisateurs du service comptabilité et les commerciaux doivent pouvoir utiliser la même imprimante EPSON05.

- Deux **groupes globaux** correspondant à ces services entreprise existent dans l'organisation, **gcompta & gcommercial**. * On crée un **groupe local de domaine DLImprimante** dans lequel on place les deux groupes globaux. * Puis on accorde au groupe **DL_Imprimante** l'autorisation d'imprimer sur **EPSON05**. ===== Les groupes prédéfinis ===== Les groupes présents après l'installation de Active Directory sont appelés « groupes prédéfinis ». Certains peuvent être gérés par l'administrateur. Voici les plus fréquemment utilisés : |Opérateurs de compte|Les membres de ce groupe peuvent administrer les comptes d'utilisateurs et les 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.| |Opérateurs de sauvegarde|Les membres de ce groupe peuvent effectuer des sauvegardes et restaurations sur tout contrôleur de domaine.| |Administrateurs|Les membres de ce groupe peuvent administrer les contrôleurs de domaine ainsi que toute station ayant intégré le domaine. Par défaut, le groupe global Administrateurs de domaine ainsi que le compte Administrateur font partie du groupe local Administrateurs.| |Invités|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.| |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. 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 Administrateurs qui lui donne ses droits.| |Contrôleurs de domaine|Ce groupe contient les comptes d'ordinateur contrôleurs de domaine du domaine. | ===== Les groupes spéciaux ===== Ces groupes ne sont pas dans la gestion des utilisateurs car 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. |Tout le monde|Comprend tous les utilisateurs, ceux que vous avez créés, le compte Invité ainsi que tous les utilisateurs des autres domaines.Attention, lorsque vous partagez une ressource, ce groupe dispose par défaut de la permission Lecture sur le partage CT pour Windows 2003).| |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.| |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.| |Réseau|Comprend toute personne accédant via le réseau à une ressource.| |Interactif|Comprend tous les utilisateurs qui ont ouvert une session localement (dans le cas où vous utilisez le « bureau à distance » ce groupe comporte tous les utilisateurs ayant ouvert une session sur le serveur de terminal).| ===== Les activités ... =====

[Je reviens à la liste des activités SISRI.](#)

From:

[/ - Les cours du BTS SIO](#)

Permanent link:

[/doku.php/reseau/ad/configserveur/gestionuser](#)

Last update: **2018/01/09 22:11**

