

La gestion des groupes sous Active directory

Les groupes de distribution.

Les groupes de distribution sont spécifiques et ne peuvent en aucun cas être associés aux permissions NTFS.

Les groupes de distribution justifient leur existence généralement pour des besoins applicatifs comme Microsoft Exchange par exemple.

Ne disposant pas de SID, aucun accès contrôlé par NTFS ne peut avoir lieu.

Les groupes de sécurité

Il est d'usage de fixer des permissions au niveau d'un groupe d'utilisateurs et non au niveau de l'utilisateur lui-même.

En effet, les groupes permettent de travailler plus efficacement en fixant des droits sur des profils (groupes), il suffit ensuite d'ajouter un utilisateur dans un groupe sans avoir à configurer complètement l'accès à une ressource.

Un utilisateur peut appartenir à plusieurs groupes.

Le cas échéant, on parle de cumul des droits.

En effet, imaginons que l'utilisateur Topper appartient au groupe Dirigeant (Lecture + Ecriture) et au groupe Qualité (Lecture seule), si l'on additionne les droits, on obtiendra des droits effectifs en Lecture + Ecriture (Lecture seule + Lecture Ecriture=Lecture Ecriture).

Il existe 4 types de groupes dont 3 au niveau AD :

- **Le groupe local (hors A.D)** : Le groupe local est stocké sur l'ordinateur où a été créé le groupe. De ce fait, il n'est pas visible sur d'autres ordinateurs.
Avant la promotion en tant que contrôleur de domaine, un serveur possède également des comptes locaux.
Les comptes locaux du serveur sont ensuite désactivés au profit des comptes de domaine.
Un groupe local peut recevoir d'autres comptes du même domaine (domaine local, groupe global, groupe universel). De cette manière, les utilisateurs du domaine peuvent se voir attribuer des permissions sur une machine cliente.
- **Le groupe de domaine local** : Les groupes locaux ne peuvent en aucun cas être utilisés en dehors du domaine où ils ont été créés. Selon les bonnes pratiques Microsoft, le groupe de domaine local sera utilisé pour recevoir éventuellement d'autres groupes et fixer des permissions d'accès.

Un groupe D.L peut recevoir : des comptes utilisateurs, des groupes globaux et universels d'un domaine quelconque de la forêt ainsi que des groupes de domaine locaux de son propre domaine.

- **Le groupe global** : Il s'agit du groupe autorisant le moins de membres. Les groupes globaux sont très souvent mis dans des groupes « Domain Local » qui possèdent les permissions (voir stratégie AGDLP). Ce groupe permet d'organiser les salariés.

Un groupe D.L peut recevoir : des comptes utilisateurs et des groupes globaux du même domaine.

- **Le groupe universel** : Le groupe universel est un peu à part puisqu'il est stocké dans le catalogue global. Si le GC est indisponible, les membres du groupe universel ne pourront pas être déterminés.

Un groupe universel peut recevoir : des comptes utilisateurs, des groupes globaux et des groupes universels d'un domaine quelconque de la forêt.

De la bonne utilisation des groupes.

Pour le néophyte, il n'est pas si facile de se repérer avec les différents types de groupe disponibles. Finalement, la meilleure méthode et de se conformer aux « best practices » de Microsoft qui a l'usage se révèlent très efficaces.

Nomenclature :

A	(Account)	Compte d'utilisateur
G	(Global Group)	Groupe Global
DL	(Domain local)	Groupe de domaine local
U	(Universal Group)	Groupe universel
P	(Permissions)	Droits NTFS

Convention de nommage :

Différencier de visu un groupe global d'un groupe de domaine local est chose impossible. Aussi, il est fortement conseillé d'utiliser des noms de groupe qui permettent de les identifier de suite.

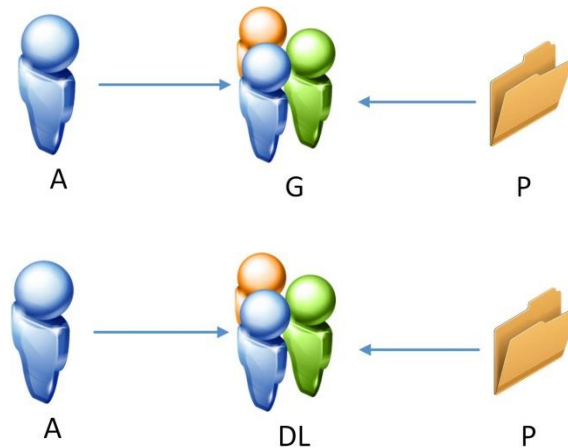
Voici quelques exemples d'utilisation :

Groupe de domaine local :	DL_Compta
Groupe Global :	GG_Compta ou G_Compta
Groupe Universel :	GU_Compta ou U_Compta

Méthode : A G P ou A DL P

Pour une architecture à domaine unique, il est possible d'utiliser 2 méthodes extrêmement rigides, qui ne conviendront pas à une évolution éventuelle de l'architecture.

Ces méthodes sont valables mais ne sont pas conseillées par Microsoft.

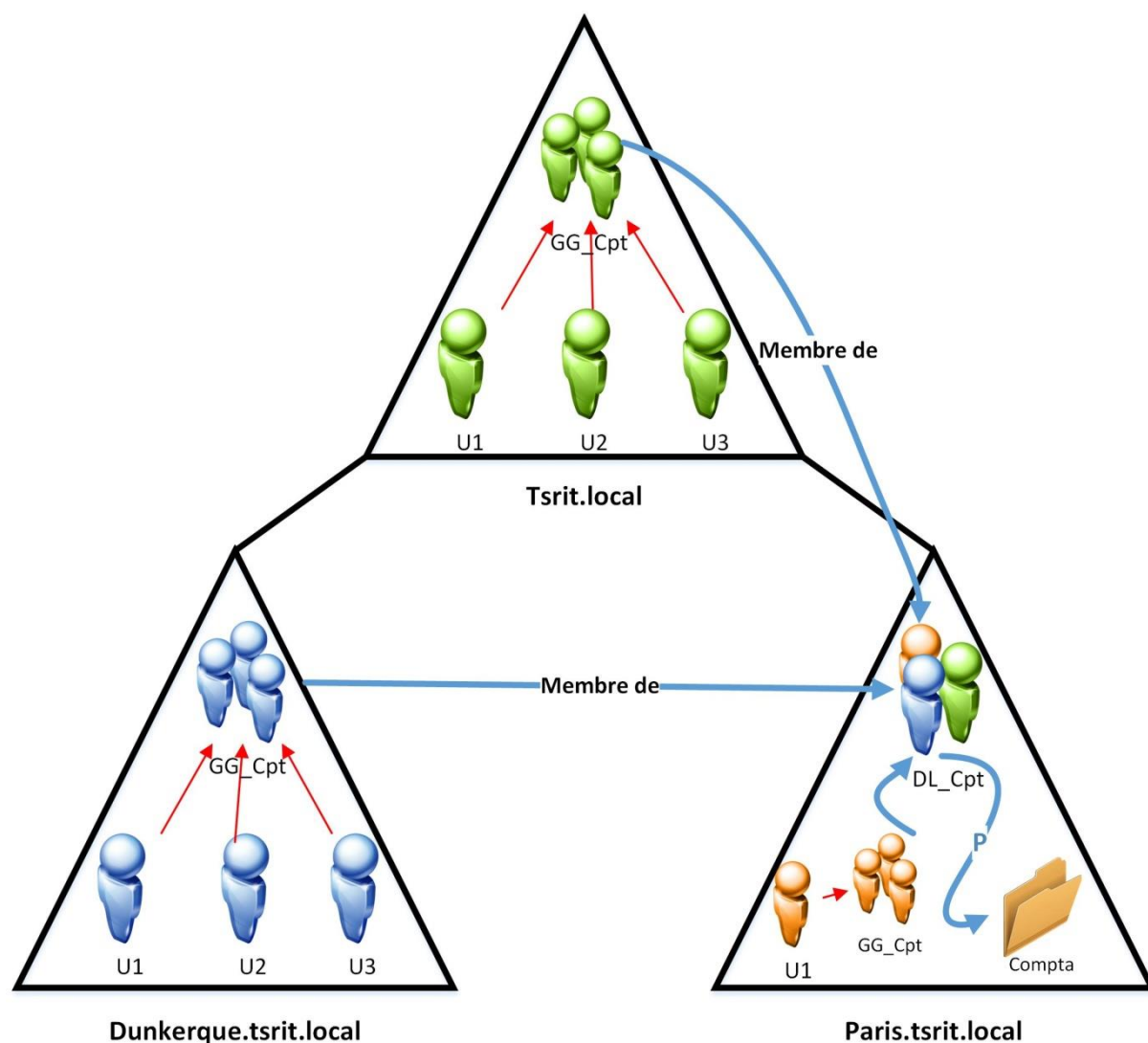


Ces méthodes, bien que déconseillées, sont simples à mettre en œuvre et sont adaptées à **une architecture à domaine unique**.

L'absence d'imbrication complexe de groupe permet de deviner facilement quels seront les droits effectifs sur le dossier.

Comme les groupes globaux n'acceptent que les comptes et les groupes globaux du même domaine, cette stratégie n'est pas adaptée au multi-domaine.

Méthode A G D L P : La formule magique !



A G D L P est LA méthode conseillée par Microsoft, adaptable à une architecture mono-domaine ou multi-domaines.

Il s'agit dans ce cas d'inclure des comptes dans un groupe local, puis d'insérer ces groupes globaux dans un groupe de domaine local pour fixer les permissions.

Cette stratégie simplifie grandement l'administration des entreprises.

Comme vous pouvez le constater sur le schéma, les permissions sont octroyées en fonction du rôle du salarié.

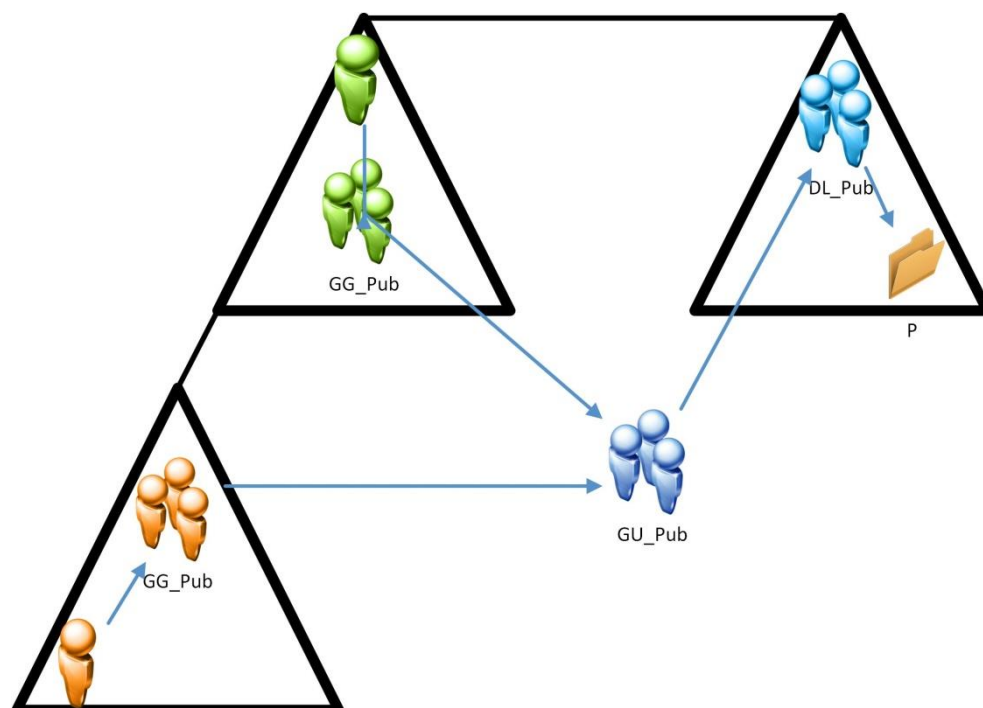
Le dossier Compta est une ressource accessible aux comptables de l'entreprise.

Généralement, les permissions sont identiques par « profil », c'est-à-dire que tous les comptables auront le même accès sur la ressource.

Si un nouveau comptable arrive dans la société, il suffira d'ajouter cet utilisateur dans le groupe global **GG_Cpt**.

Bien que cette méthode simplifie l'administration d'une entreprise, elle est réservée aux structures qui gèrent de nombreux utilisateurs.

Méthode A G U D L P : Pour les très grands réseaux



Pour utiliser les groupes universels, votre forêt doit fonctionner en mode natif Windows 2000 au minimum.

Cette méthode est réservée aux entreprises de très grande ampleur, possédant une architecture multi-domaine et regroupant des centaines d'utilisateurs.

Cette méthode permet de limiter le nombre de groupes dans le groupe Domain Local.