- Le SID correspondant au groupe Administrateurs est celui-ci : S-1-5-32-544.
- L'autorité ayant émis ce SID a pour identifiant le chiffre 5.
- La sous-autorité a pour identifiant le nombre 32.
- 544 est le RID du groupe Administrateurs.

Vous pouvez tester les résultats affichés par ces autres commandes :

- `whoami`
- `whoami /user /priv`
- `whoami /groups`

Les privilèges de l'utilisateur actuellement connecté seront affichés. Vous pouvez obtenir certains SID des utilisateurs ou des entités de sécurité en ouvrant cette arborescence du Registre : **HKEY_LOCAL_MACHINE - SOFTWARE - Microsoft - Windows NT - CurrentVersion - ProfileList**.

Enfin, les SID de certaines entités intégrées sont visibles dans cette autre arborescence : HKEY_USERS.

2. Les listes de contrôle d'accès

Une liste de contrôle d'accès discrétionnaire (DACL ou *Discretionary Access Control Lists*, plus communément appelée ACL) est un mécanisme permettant de protéger des ressources telles que les fichiers et les clés du Registre. Les DACL contiennent des entrées de contrôles d'accès (ACE ou *Access Control Entry*) qui fonctionnent comme des enregistrements pour chaque utilisateur ou groupe d'utilisateurs désigné par son SID. Ces entrées associent une entité de sécurité (un compte d'utilisateur, un groupe de comptes, une entité système) à une règle définissant l'utilisation de la ressource. Les DACL et les ACE vous permettent d'accorder ou de refuser des droits aux ressources selon les autorisations que vous voulez associer aux comptes d'utilisateurs. Vous pouvez ainsi créer une ACE et l'appliquer à la DACL d'un fichier pour empêcher quiconque, à l'exception d'un administrateur, de modifier ce fichier.

Une liste de contrôle d'accès système (SACL ou "ACE d'audit") est un mécanisme qui contrôle les messages d'audit associés à une ressource. Les SACL contiennent des ACE qui définissent les règles d'audit pour une ressource donnée.

Vous pouvez donc utiliser les DACL pour vous assurer que seul un administrateur peut modifier un fichier ; et les SACL pour vous assurer que toutes les tentatives d'ouverture d'un fichier qui aboutissent sont enregistrées. Il est courant de distinguer les ACE positives des ACE négatives :

- Dans l'Explorateur Windows, ouvrez votre répertoire d'utilisateur.
- Créez un nouveau dossier nommé *Test*.
- Effectuez un clic droit puis cliquez sur le sous-menu **Propriétés**.
- Cliquez sur l'onglet **Sécurité**.

Notez que les ACE ou autorisations qui sont visibles sont toutes grisées puisqu'elles héritent du dossier parent.