**Une liste de SID**

Le SID (Security identifier) est une valeur unique qui est utilisée pour identifier un utilisateur ou un groupe du système d'exploitation Windows.

|  |  |
| --- | --- |
| **SID** | **Utilisateur** |
| **S-1-5-21**-<nombre>-<nombre>-<nombre>-**500** | **Administrateur**  ou  **Administrator** |

|  |  |
| --- | --- |
| **SID** | **Groupe** |
| **S-1-5-32-544** | **Administrateurs**  ou  **Administrators** |
| **S-1-5-32-545** | **Utilisateurs**  ou  **Users** |
| **S-1-5-21**-<nombre>-<nombre>-<nombre>-**512** | **Admins du domaine**  ou  **Domain Admins** |
| **S-1-5-21**-<nombre>-<nombre>-<nombre>-**513** | **Utilisateurs du domaine**  ou  **Domain Users** |
| **S-1-5-21**-<nombre>-<nombre>-<nombre>-**515** | **Ordinateurs du domaine**  ou  **Domain Computers** |
| **S-1-5-21**-<nombre>-<nombre>-<nombre>-**516** | **Contrôleurs de domaine**  ou  **Domain Controllers** |

|  |  |
| --- | --- |
| **SID** | **Principaux de sécurité intégrés** |
| **S-1-1-0** | **Tout le monde**  ou  **Everyone** |
| **S-1-3-4** | **DROITS DU PROPRIÉTAIRE**  ou  **OWNER RIGHTS** |
| **S-1-5-11** | **Utilisateurs authentifiés**  ou  **Authenticated Users** |
| **S-1-5-18** | **Système**  ou  **SYSTEM** |

**# Commande pour afficher la valeur S-1-5-21-<nombre>-<nombre>-<nombre> d'un domaine**

**(Get-ADDomain).DomainSID.Value**

On peut savoir si un utilisateur a ouvert l'invite de commandes avec une élévation des autorisations.

En exécutant la commande suivante "**whoami.exe /all**" et en vérifiant la valeur du SID.

|  |  |
| --- | --- |
| **SID** | **Interprétation du SID** |
| S-1-16-8192 | Autorisations standard |
| S-1-16-12288 | Élévation des autorisations |