**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 ou Groupe** |
| S-1-1-0 | Tout le monde |
| S-1-3-0 | CREATEUR PROPRIETAIRE |
| S-1-3-1 | GROUPE CREATEUR |
| **S-1-3-4** | **DROITS DU PROPRIÉTAIRE** |
| S-1-5 | NT AUTHORITY |
| S-1-5-1 | LIGNE |
| S-1-5-2 | RESEAU |
| S-1-5-3 | TACHE |
| S-1-5-4 | INTERACTIF |
| S-1-5-6 | SERVICE |
| S-1-5-7 | ANONYMOUS LOGON |
| **S-1-5-11** | **Utilisateurs authentifiés** |
| S-1-5-13 | UTILISATEUR TERMINAL SERVER |
| S-1-5-14 | REMOTE INTERACTIVE LOGON |
| **S-1-5-18** | **SYSTEM** |
| S-1-5-19 | SERVICE LOCAL |
| S-1-5-20 | SERVICE RÉSEAU |
| **S-1-5-21**-<nombre>-<nombre>-<nombre>-**500** | **Administrateur** |
| S-1-5-21-<nombre>-<nombre>-<nombre>-501 | Invité |
| **S-1-5-32-544** | **Administrateurs** |
| S-1-5-32-545 | Utilisateurs |
| S-1-5-32-546 | Invités |
| S-1-5-32-547 | Utilisateurs avec pouvoir |
| S-1-5-32-551 | Opérateurs de sauvegarde |
| S-1-5-32-552 | Duplicateurs |
| S-1-5-32-555 | Utilisateurs du Bureau à distance |
| S-1-5-32-556 | Opérateurs de configuration réseau |

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 |