SID (*Security Identifier*)

Pour identifier les ressources et les personnes sur une machine locale ou sur un réseau, Windows repose sur l'emploi de valeurs spéciales, nommées identifiants de sécurité (SID, Security Identifiers), qui sont à la source d'un moyen commode de distinguer sans ambiguïté les entités d'un système. Les utilisateurs et leurs processus, les groupes locaux, les groupes de domaine, les ordinateurs locaux, les domaines et membres de domaine, tout ce qui peut être authentifié par le système d'exploitation a un SID qui lui est associé. L'environnement Microsoft se base sur cette information chaque fois qu'il est nécessaire de réaliser des contrôles d'accès, par exemple pour réaliser une ouverture de session locale ou ouvrir des sessions vers le domaine.

Les SID existent depuis la toute première version de Windows NT et constituent une pierre angulaire importante de la protection de ces systèmes. Les algorithmes liés fonctionnent en lien avec des composants spécifiques de l'autorisation qui, pensés pour fournir un environnement informatique plus sécurisé, agissent dès qu'il est question de vérifier si une entité demandant d'accéder à une ressource a les droits nécessaires pour le faire.

Chaque SID se présente sous forme d'une chaine alphanumérique construite en partie sur le principe de l'imprévisibilité, d'où le caractère unique de chaque représentation. Étant donnée l'étendue que peut couvrir un SID (il s'agit généralement d'un nombre très grand), couplé au fait que Windows génère des valeurs purement aléatoires au sein de chaque SID, il est virtuellement impossible à Windows d'émettre le même SID deux fois sur des machines ou des domaines de par le monde. Il est plus efficace pour le système d'exploitation d'utiliser le SID, plutôt que le nom, pour identifier un utilisateur (ou toute autre personnification) car les noms, susceptibles déjà de ne pas être uniques, peuvent en outre être modifiés.

Au plus haut niveau d'abstraction, un SID est une valeur numérique de longueur variable qui se compose d'un numéro de révision, d'une valeur autorité identificatrice sur 48 bits et d'un certain nombre de valeurs de valeurs sous-autorité sur 32 bits. Les valeurs individuelles d'un SID correspondent donc à ceci :

- **Révision** Indique la version de la structure de données (format binaire) SID qui est utilisée dans un SID spécifique. La structure employée par Windows jusqu'à ce jour comporte un numéro de révision égal à 1.
- **Autorité identificatrice** Identifie l'agent émetteur du SID, généralement un système local ou un domaine Windows.
- **Sous-autorités** Identifie les sous-autorités de confiance (RID, Relative ID) relatives à l'autorité ayant produit le SID. Les RID désignent des comptes ou groupes à l'intérieur d'un domaine. L'identifiant RID est unique seulement au sein d'un domaine, tandis que le SID, de par ses aspects cumulatifs, est unique dans toutes les installations de Windows.

Les composants d'un SID sont plus faciles à visualiser lorsque les SID sont converties à partir d'un fichier binaire dans un format de chaîne à l'aide de la notation standard, soit S-R-X-Y1-Y2-Yn. Dans cette notation, la lettre S sert à montrer que la série alphanumérique qui suit est

un SID, R représente un numéro de révision, X indique la valeur autorité et Y une série de valeurs sous-autorité, où n est le nombre de valeurs. L'exemple suivant est à considérer :

Dans ce SID, le numéro de révision est 1 et la valeur de l'autorité identificatrice est 5 (autorité de sécurité Windows) ; le reste du SID est composé de deux valeurs de sous-autorité : 32 (SECURITY_BUILTIN_DOMAIN_RID) et 544 (DOMAIN_ALIAS_RID_ADMINS).

Lorsque vous installez Windows, le programme d'installation émet un SID pour l'ordinateur, de sorte qu'il est impossible pour deux ordinateurs du réseau d'avoir le même SID.

Windows assigne des SID aux comptes locaux de la machine. Lorsque vous créez un compte d'utilisateur ou de groupe, Windows lui assigne un SID unique, lequel reste associé à ce seul compte jusqu'à sa suppression. Si vous renommez un compte, le SID ne change pas, et tous les attributs afférents (droits et autres autorisations) sont préservés. Si vous supprimez un compte , toutes les attributions de sécurité associées à ce compte sont également supprimées. Windows ne réutilisant pas le SID qui était attribué à un compte, même si des comptes partagent le même nom, ils ne partagent pas le même SID. Chaque SID de compte local est basé sur le SID de l'ordinateur source et a un RID à la fin. Les RID des comptes utilisateur et des groupes commencent à 1000 et augmentent de 1 pour chaque nouvel utilisateur ou groupe.

Pour les quelques comptes créés automatiquement lors de l'installation du système, Windows crée des SID qui se composent d'un SID de machine ou de domaine complété par un RID prédéfini. Par exemple, le RID du compte Administrateur est 500 et le RID du compte Invité est 501. Le compte administrateur local d'un ordinateur a comme base le SID machine, auquel s'ajoute le RID 500. Cela donne :

S-1-5-21-2647556361-93858140-2277411872-500

Les valeurs de RID inférieures à 1000 sont destinées à un usage interne de la part du système d'exploitation, qui les utilise dans ce contexte pour identifier des sujets connus. Les comptes d'utilisateurs créés par la suite reçoivent des RID dont la valeur de départ est fixée à 1000.

Enfin, Winlogon créee un SID unique pour chaque session interactive. Le SID d'une session interactive est de la forme S-1-5-5-0, complétée par un RID généré aléatoirement.

Les principales interfaces que fournit Windows en matière de SID incluent AllocateAndInitializeSid, CreateWellKnownSi, GetLengthSid, LookupAccountSid, ConvertSidToStringSid.

En pratique : visualisation des SID de compte

L'utilitaire PsGetSid permet de traduire les noms des comptes de machine et d'utilisateur en les SID associés, et vice-versa.

Si vous exécutez PsGetSid sans options, il affiche le SID assigné à l'ordinateur local.

```
c:\>psgetsid

SID for \\lain:
S-1-5-21-495418598-4048141043-142412758
```

Pour connaitre le SID d'un compte d'utilisateur, spécifiez le nom de l'utilisateur comme argument de PsGetSid :

```
c:\>psgetsid

SID for lain\arnaud:
S-1-5-21-495418598-4048141043-142412758-1002
```

Il est également facile de voir la représentation SID de vos comptes avec l'utilitaire Whoami.

Pour afficher le SID de l'utilisateur actuellement connecté sur le système local, saisissez whoami /user.

Afin d'afficher les identificateurs des groupes, saisissez : whoami /groups.

Pour afficher le nom de l'utilisateur actuel, les groupes auxquels il appartient ainsi que les SID et les privilèges de l'utilisateur actuel, saisissez : whoami /all.

Une autre possibilité en ce qui concerne la lecture des SID repose sur l'utilisation de la console WMI, où l'alias useraccount fournit une passerelle vers la gestion des comptes. Pour afficher les noms et les SID des utilisateurs locaux, saisissez la commande wmic useraccount get name,sid. Vous devriez vois quelque chose ressemblant à ce qui suit :

```
C:\>wmic useraccount get name,sid
Name            SID
Administrateur  S-1-5-21-495418598-4048141043-142412758-500
arnaud          S-1-5-21-495418598-4048141043-142412758-1002
Invité          S-1-5-21-495418598-4048141043-142412758-501
```

La raison principale pour Windows d'utiliser des SID, plutôt que des noms, afin de répertorier les diverses entités établies dans le modèle de sécurité réside dans l'impossibilité de donner aux noms un caractère définitif et irréversible, ainsi que de leur faire porter une grande quantité d'informations. Les noms de compte et les noms complets associés à des utilisateurs peuvent par exemple être modifiés, soit par décision de l'administrateur, soit s'il dispose des droits nécessaires pour le faire, par l'utilisateur lui-même. À plus grande échelle, quand un ensemble de machines se partagent des informations d'annuaire (domaine), les noms seuls ne peuvent servir à faire la différence entre comptes et groupes (un groupe d'utilisateurs est un ensemble de comptes d'utilisateurs) : une machine peut par exemple abriter un compte d'utilisateur x, et une autre machine un groupe homonyme. (Notez que pour éviter toute confusion, Windows interdit que les comptes locaux d'une machine aient le même nom). En outre, du fait de la prise en compte de solutions multilingues, certaines désignations varient d'un système à l'autre. Par exemple, toutes les versions américaines standard de Windows (anglais américain) sont distribuées avec un groupe prédéfini nommé Administrators et dont le SID est S-1-5-32-544. Sur les systèmes en langue française, le même groupe est appelé Administrateurs.