Dans un environnement Active Directory, un identificateur de sécurité, *security identifier* (SID) en anglais, est un identifiant unique attribué à chaque objet de sécurité, tels que les utilisateurs, les groupes et les ordinateurs. Il est utilisé pour identifier de manière univoque un objet au sein du domaine Active Directory et pour contrôler l'accès aux ressources et aux données.

Les identificateurs de sécurité sont largement utilisés dans la gestion des autorisations et des droits d'accès. Lorsqu'un utilisateur ou un groupe se voit accorder des autorisations sur des ressources telles que des fichiers, des dossiers ou des imprimantes, leurs identificateurs de sécurité sont enregistrés dans les listes de contrôle d'accès associées à ces ressources. Ils sont également présents dans les descripteurs de sécurité, *security descriptor* en anglais, et les jetons d’accès, *access token* en anglais.

Un utilisateur peut avoir plus d’un identificateur de sécurité. Si l’utilisateur fait partie de groupes, celui-ci aura également les identificateurs de sécurité de ces groupes. Lors de la connexion de l’utilisateur sur un système Windows, celui-ci aura également un identificateur de sécurité pour sa session Windows.

Les identificateurs de sécurité conservent leur unicité et leur validité à travers le réseau, ce qui signifie qu'ils peuvent être utilisés pour contrôler l'accès aux ressources partagées sur différents ordinateurs et serveurs dans le domaine Active Directory.

De plus, identificateurs de sécurité sont persistants, ce qui signifie qu'ils ne changent pas, même si le nom de l'objet associé est modifié. Cela garantit que les autorisations accordées à un objet restent cohérentes même en cas de changement de nom. À noter qu’Ils peuvent cependant changer lors d’une migration vers un autre domaine ou une autre forêt Active Directory.

L’identificateur de sécurité est inscrit dans l’attribut "objectSID". Il se présente sous la forme d’une chaine de caractères composée de six parties, séparées par des tirets (-) :

* Le caractère "S", qui indique que la chaine de caractères est un identificateur de sécurité
* Le niveau de révision, exemple "1"
* La valeur de l’autorité d’identificateur, exemple "5"
* La série de valeurs de sous-autorités, exemple "21"
* L’identifiant du domaine, exemple : "602238038-4219226198-393252848"
* L’identifiant relatif de l’objet, exemple : "500" pour le compte administrateur par défaut du domaine

Exemple de l’identificateur de sécurité du compte administrateur par défaut d’un domaine Active Directory : " S-1-5-21-602238038-4219226198-393252848-500".

En résumé, les Identificateurs de sécurité sont des composants fondamentaux de la gestion des accès et de la sécurité dans un environnement Active Directory, fournissant une manière unique et persistante d'identifier les objets de sécurité et de contrôler leur accès aux ressources.

Documentation :

* <https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/understand-security-identifiers>