Las cuentas de ordenador, cuentas de usuario, grupos y otros objetos relacionados con la seguridad son principios de seguridad. Los identificadores de seguridad (SID) identifican de manera única los principios de seguridad.

Cada vez que Windows y Active Directory crean un principio de seguridad, generan un SID para él. La Autoridad de seguridad local de Windows (LSA) genera SID para los principios de seguridad local que luego los almacena en la base de datos de seguridad local.

La autoridad de seguridad del dominio genera SID para los principios de seguridad del dominio y luego los almacena en Active Directory. Los SID son únicos dentro de su alcance.

El SID de cada principio de seguridad local es único en la ordenador, y el SID de cada principio de seguridad de dominio es único dentro de cualquier dominio de la empresa. Además, Windows y Active Directory nunca vuelven a usar un SID, incluso si eliminan el principio de seguridad al que pertenecía ese SID. Por lo tanto, si elimina una cuenta y luego la vuelve a agregar, la cuenta obtiene un nuevo SID.

Lo importante para recordar es que cada cuenta tiene un SID. Es como tener un número de pasaporte que lo identifica de manera única a la inmigración. Puede referirse a una cuenta por su nombre o por su SID, pero en la práctica rara vez utiliza el SID porque su formato es engorroso. Sin embargo, frecuentemente ve los SID de las cuentas en el registro.

Un ejemplo de un SID es S-1-5-21-2857466466-1465059943-1690550265-500. Un SID siempre comienza con S-. El siguiente número identifica la versión del SID, en este caso, la versión 1. El siguiente número indica la autoridad del identificador y suele ser 5, que es NT Authority.

La cadena de números hasta 500 es el identificador de dominio, y el resto del SID es un identificador relativo, que es la cuenta o grupo. Esta es una descripción muy aproximada del formato SID, que es mucho más complejo de lo que caracteriza el anterior ejemplo mostrado.

Algunos SID, como S-1-5-18, son más cortos que el del ejemplo anterior. Estos son SID conocidos, y son los mismos en todas las ordenador y en todos los dominios. Son interesantes porque aparecen una y otra vez en el registro y en otros lugares.

A continuación muestro una serie de SID que describe los SID bien conocidos por Windows. El dominio de marcador de posición es el identificador de dominio del SID.

SID	User o Nombre de Grupo
S-1-0	Null Authority
S-1-0-0	Nobody
S-1-1	World Authority
S-1-1-0	Everyone
S-1-2	Local Authority
S-1-2-0	Local
S-1-3	Creator
S-1-3-0	Creator Owner
S-1-3-1	Creator Group
S-1-3-2	Creator Owner Server
S-1-3-3	Creator Owner Group
S-1-4	Nonunique Authority
S-1-5	NT Authority
S-1-5-1	Dialup
S-1-5-2	Network
S-1-5-3	Batch
S-1-5-4	Interactive
S-1-5-5-X-Y	Logon Session
S-1-5-6	Service
S-1-5-7	Anonymous
S-1-5-8	Proxy

S-1-5-9	Enterprise Domain Controllers
S-1-5-10	Self
S-1-5-11	Authenticated Users
S-1-5-12	Restricted
S-1-5-13	Terminal Service User
S-1-5-14	Remote Interactive Logon
S-1-5-18	LocalSystem or System
S-1-5-19	LocalService
S-1-5-20	NetworkService
S-1-5-domain-500	Administrator
S-1-5-domain-501	Guest
S-1-5-domain-502	krbtgt
S-1-5-domain-512	Domain Admins
S-1-5-domain-513	Domain Users
S-1-5-domain-514	Domain Guests
S-1-5-domain-515	Domain Computers
S-1-5-domain-516	Domain Controllers
S-1-5-domain-517	Cert Publishers
S-1-5-root domain-518	Schema Admins
S-1-5-root domain-519	Enterprise Admins
S-1-5-root domain-520	Group Policy Creator Owners
S-1-5-domain-553	RAS and IAS Servers
S-1-5-32-544	Administrators
S-1-5-32-545	Users
S-1-5-32-546	Guests
S-1-5-32-547	Power Users
S-1-5-32-548	Account Operators
S-1-5-32-549	Server Operators
S-1-5-32-550	Print Operators
S-1-5-32-551	Backup Operators
S-1-5-32-552	Replicator
S-1-5-32-554	Pre-Windows 2000 Compatible Access
S-1-5-32-555	Remote Desktop Users
S-1-5-32-556	Network Configuration Operators

S-1-6	Site Server Authority
S-1-7	Internet Site Authority
S-1-8	Exchange Authority
S-1-9	Resource Manager Authority