How do I convert a SID between binary and string forms?

devblogs.microsoft.com/oldnewthing/20040315-00

March 15, 2004

Raymond Chen

Of course, if you want to do this programmatically, you would use ConvertSidToStringSid and ConvertStringSidtoSid, but often you're studying a memory dump or otherwise need to do the conversion manually. If you have a SID like S-a-b-c-d-e-f-g-... Then the bytes are

a	(revision)
N	(number of dashes minus two)
bbbbbb	(six bytes of "b" treated as a 48-bit number in big-endian format)
cccc	(four bytes of "c" treated as a 32-bit number in little-endian format)
dddd	(four bytes of "d" treated as a 32-bit number in little-endian format)
eeee	(four bytes of "e" treated as a 32-bit number in little-endian format)
ffff	(four bytes of "f" treated as a 32-bit number in little-endian format)
etc.	

So for example, if your SID is `S-1-5-21-2127521184-1604012920-1887927527-72713`, then your raw hex SID is 010500000000000515000000A065CF7E784B9B5FE77C8770091C0100 This breaks down as follows:

01	S-1
05	(seven dashes, seven minus two = 5)
000000000005	(5 = 0x000000000005, big-endian)
15000000	(21 = 0x00000015, little-endian)
A065CF7E	(2127521184 = 0x7ECF65A0, little-endian)

784B9B5F	(1604012920 = 0x5F9B4B78, little-endian)
E77C8770	(1887927527 = 0X70877CE7, little-endian)
091C0100	(72713 = 0x00011c09, little-endian)

Yeah, that’s great, Raymond, but what do all those numbers mean?

S-1-	version number (SID_REVISION)
-5-	SECURITY_NT_AUTHORITY
-21-	SECURITY_NT_NON_UNIQUE
-…-…-…-	these identify the machine that issued the SID
72713	unique user id on the machine

Each machine generates a unique ID that it uses to stamp all the SIDs it creates (-…-…-…-). The last number is a “relative id (RID)” that represents a user created by that machine. There are a bunch of predefined RIDs; you can see them in the header file ntseapi.h, which is also where I got these names from. The system reserves RIDs up to 999, so the first non-builtin account gets assigned ID number 1000. The number 72713 means that this particular SID is the 71714th SID created by the issuer. (The machine that issued this SID is clearly a domain controller, responsible for creating the accounts of tens of thousands of users.) (Actually, I lied above when I said that this is the 71714th SID created by the issuer. Large servers can delegate SID creation to helpers, in which case SID issuance is no longer strictly consecutive.)

Security isn’t my area of expertise, so it’s entirely possibly (perhaps even likely) that I got something wrong up above. But it’s mostly correct, I think.

Raymond Chen

Follow