Detecting whether a SID is well-known SID

devblogs.microsoft.com/oldnewthing/20141212-00

December 12, 2014

Raymond Chen

You might think that the `IsWellKnownSid` function would tell you whether a SID is well-known, but it doesn't. Rather, it tells you whether a SID exactly matches the well-known SID you specified. For example, you can ask, "Is this the *Authenticated Users* SID?" or "Is this the *Everyone* SID?" But you can't ask, "Is this any type of well-known SID?"

I guess you could enumerate through all the well-known SIDs, and check if your SID matches any of them, but that's getting kind of ugly.

If what you're interested in is whether this is a machine-relative SID (or a domain-relative SID, which is the special case where the machine is the domain controller), as opposed to a universal SID, you can check whether the SID format is S-1-5-**21**-#-#-#-#. All machine-relative SIDs have that form.

```
#define SECURITY_NT_NON_UNIQUE          (0x00000015L) // decimal 21
#define SECURITY_NT_NON_UNIQUE_SUB_AUTH_COUNT  (3L)
```

If you want to exclude `machine\Administrator` and other predefined machine-relative SIDs, you can verify that the last number (the RID) is greater than or equal to 1000.

```
#define SECURITY_OTHER_ORGANIZATION_RID (0x000003E8L)
```

Raymond Chen

Follow