

Why did the friendly name for the Network Service account change?

devblogs.microsoft.com/oldnewthing/20160519-00

May 19, 2016



Raymond Chen

A customer had a service that runs under the Network Service account. They found that starting in Windows Vista, if the service calls `GetUserName`, it no longer gets “NETWORK SERVICE” back; instead, it gets the computer name followed by a dollar sign. Why did this change?

Well, nobody promised that it wouldn’t change.

Whether the name for the Network Service account is “NETWORK SERVICE” or “HOSTNAME\$” depends on a variety of things, including whether the service is authenticated with Active Directory (in which case it presents itself to the Active Directory server as the machine name).

The customer requires official documentation for the change. Is there a document available that explains the change and why it occurred?

The customer should not be relying on account display names in the first place. If you want to identify an account, use the SID. The SID is fixed and documented as S-1-5-20. The display name is neither fixed nor documented.

The fact that their service is sensitive to the display name for the Network Service kind of scares me, because it suggests that if I change my display name to “NETWORK SERVICE” (my friends call me Netty for short), their service might treat me as if I’m the Network Service account, and now I’ve gained service privileges. Little Bobby Tables, eat your heart out!

The customer liaison explained,

The customer’s application was designed to use both user names and SIDs, and they found that their design stopped working. Now they need to redesign their application, but they need to justify the work on their side, hence their request for formal documentation confirming the change.

Okay, so they want the document in order to make themselves look good. “See, Microsoft made a change and screwed us. That’s why we have this unexpected work.”

Their design relied on undocumented behavior. Undocumented behavior can change at any time. This is one example of undocumented behavior changing. If we had to document every undocumented behavior, then it wouldn’t be undocumented any more.

This specific change was an internal change that does not need to be documented externally because properly-written code should not have been relying on it. Any documentation that could be written on the subject would continue to be non-contractual because Windows is within its rights to change the behavior at any time without warning.

I don’t know what happened next, but it looks like the customer eventually pressured somebody into documenting it, because a paragraph addressing this specific issue was added to the documentation for the GetUserName function. MSDN is being used as a pawn in some company’s internal politics.

I suspect the need for that sentence is now gone, so I need to file a documentation change request to replace that sentence with “Applications should use SIDs to identify well-known accounts rather than display names.”

Raymond Chen

Follow

