How can I detect that a user's SID has changed and recover their old data?

devblogs.microsoft.com/oldnewthing/20140829-00

August 29, 2014

Raymond Chen

A customer maintained a database which recorded information per user. The information in the database is keyed by the user's SID. This works out great most of the time, but there are cases in which a user's SID can change. "Wait, I thought SIDs don't change." While it's true that SIDs don't change, it is also true that the SID associated with a user can change. Since SIDs encode the domain to which they belong, a user which moves from one domain to another within an organization, will need to be assigned a new SID. But wait, does that mean that the user lost access to all their stuff? After all, all their stuff was marked "Owned by X\UserName" but the user's SID is now Y\UserName. No, the user doesn't lose access to their stuff thanks to SID history, and if you move users around a lot, the SID history can get quite large. A token for a user contains not only their current identity but also all of their earlier identities. That is what permits Y\UserName to continue to access things that was marked "Owned by X\UserName": The token for Y\UserName includes an entry that says, "Oh, I used to be X\UserName." The customer's database can take advantage of the SID history to match up users with their former selves. Our customer was lucky in that their database recorded only users who had logged into the local machine, so that list is typically pretty small. The simplest solution for this particular customer is just to go through all the users in the database, and for each one, see if the current user has that database user in their SID history. And the easy way to do that is to make the security system do the work for you: To see if the current user has user X in their SID history, create a security descriptor that grants access only to user X, then call `AccessCheck` to see if the current user can access it. If so, then that means that the current user was at one point in the past known as X.

(If you have a large database where iterating over all users is impractical, you can ask for the current user's SID-History attribute and walk through the previous identities manually.)

Raymond Chen

Follow