

Re: Unexplained User Account Deletion

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-12/msg01215

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxx>
 - *Date:* Sat, 16 Dec 2006 12:33:33 -0500
-

What you mean generates a modified GUID? The object GUID does not change during a "delete", it is maintained through the tombstone process.

--

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

michael_gore718@xxxxxxxxxx wrote:

So here's an iffy one. Turns out a user account was deleted and everything is pointing towards me. However I don't recall deleting the

account, then confirming the deletion, and confirming the deletion of the associated mailbox. Heres the info from the Event logs, the header

is the same for both events:

Header>>

Date: 12/13/06
Source: Security
Time: 4:18:35 PM
Category: Account Mgmt
Type: Success A
Event ID: 630

This is the event in question>>

Re: Unexplained User Account Deletion

User Account Deleted:
Target Account Name: User1
Target Domain: DOMAIN
Target Account ID: DOMAIN\User1
Caller User Name: admin
Caller Domain: DOMAIN
Caller Logon ID: (0x0,0x64390BE)
Privileges: -

Here is the account I was working on at the time>>>

User Account Deleted:
Target Account Name: User2
Target Domain: DOMAIN
Target Account ID: User2
DEL:d006b3a0-09de-45f2-8393-ba47246b8ea8
Caller User Name: admin
Caller Domain: DOMAIN
Caller Logon ID: (0x0,0x64390BE)
Privileges:

Right off the back i'm sure you can tell that something is missing.
WHERE IS THE GUID? It's been my experience that a deleted account
generates a modified GUID. Im not sure why the GUID was not generated
in the event. Can anyone explain this?

Another bit of information, the two events were timestamped for exactly

4:18:35 PM. Any help on this will be appreciated.